REPORT
CONCERNING THE ATTORNEY GENERAL'S RENEWED DETERMINATION THAT THE UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND, AND THE 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 CRIME, SATISFY THE REQUIREMENTS OF 18 U.S.C. § 2523(b)

AS REQUIRED BY SECTION 2523(e)(2) OF THE CLARIFYING LAWFUL OVERSEAS USE OF DATA ACT

SUBMITTED TO THE COMMITTEES ON THE JUDICIARY AND FOREIGN RELATIONS OF THE UNITED STATES SENATE AND THE COMMITTEES ON THE JUDICIARY AND FOREIGN AFFAIRS OF THE UNITED STATES HOUSE OF REPRESENTATIVES

November 2024

I. Introduction

The Clarifying Lawful Overseas Use of Data Act, codified at Title 18, United States Code, Section 2523 (the "CLOUD Act" or "Act"), sets out requirements and procedures for entering into cross-border data access executive agreements. Section 2523(e) requires that, every five years, the Attorney General review and, in his discretion, with the concurrence of the Secretary of State, renew the determination that the requirements of Section 2523(b) of the Act are satisfied. Upon renewal of the determination, Section 2523(e) directs the Attorney General to transmit a report to the Committees on the Judiciary and on Foreign Relations of the Senate and on the Judiciary and on Foreign Affairs of the House of Representatives describing: the reasons for the renewal; any substantive changes to the Agreement or relevant laws and procedures in the partner country; and the implementation of the Agreement, including problems or controversies arising as a result of the agreement or its implementation.

On October 3, 2019, the United States signed the 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 Crime (the "U.S.-UK Agreement" or "Agreement"), the first executive agreement authorized under the CLOUD Act. On November 27, 2019, then Attorney General William Barr certified his determination that both the United Kingdom of Great Britain and Northern Ireland (the "United Kingdom" or "UK") and the Agreement satisfied the requirements of Section 2523(b) of the Act, and that the Secretary of State concurred in this determination. Thereafter, the Department of Justice notified Congress of the Attorney General's certification of the Agreement, as required by Section 2523(d)(1) of the Act. Congress took no action to disapprove the Agreement, and it entered into force on October 3, 2022. The Agreement, by its terms, will expire on October 3, 2027, unless renewed by both countries for a further five years through the exchange of diplomatic notes.[1]

Pursuant to Section 2523(e)(1) of the Act, with the concurrence of the Secretary of State, the Attorney General has fully reviewed the considerations specified in Section 2523(b) of the Act and renewed the determination that the United Kingdom and the Agreement meet the requirements of Section 2523(b).[2] Accordingly, pursuant to Section 2523(e)(2) of the Act, the Department of Justice submits this report.

II. Reasons for Renewal

The United Kingdom's laws and procedures continue to meet the requirements of Section 2523(b) based on the considerations set forth in paragraphs (1), (2), (3), and (4) of Section 2523(b) as discussed in the Explanation of Each Consideration in Determining that the Agreement Satisfies the Requirements of 18 U.S.C. § 2523(b) (the "2019 Explanation") which

---

[1] *See* Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime, U.K.-U.S., art. 17(1), Oct. 3, 2019, 60 I.L.M. 171.

[2] A certification of the renewal of this determination will be published in the Federal Register pursuant to 18 U.S.C. § 2523(g).

accompanied then-Attorney General Barr's certification of the Agreement in 2019. There have been no changes to the Agreement's terms, and, as set forth below, any relevant, substantive changes to the domestic laws of the United Kingdom are consistent with CLOUD Act requirements. Further, the United Kingdom has appropriate processes and procedures to implement the requirements of the U.S.-UK Agreement.

Significantly, the United Kingdom has reported that, during its two-year operation, the Agreement has served as an important tool for UK authorities, contributing to their successful efforts to combat serious crime, including terrorism. UK authorities report that between January and July 2024, the Agreement has contributed directly to 368 arrests, the seizure of 3.5 tons of illicit drugs, the recovery of GBP 5 million, the seizure of 94 firearms and 745 rounds of ammunition, and the identification of 41 threats to life and 100 threats of harm. Although, as anticipated, United States cases have not given rise to as many requests under the Agreement, U.S. authorities have nonetheless used the Agreement to secure electronic data in an expedited manner to further investigations against computer intrusion, fraud, money laundering, threats and extortion, tax offenses, and customs violations, among other criminal activity.

III. Changes to the Agreement and the Relevant Laws and Procedures of the United Kingdom

The United States and the United Kingdom have not negotiated or agreed to any changes to the terms of the U.S.-UK Agreement since its certification to Congress. However, in the interim, there have been some legal developments in the United Kingdom relating to data protection, online harms, and investigatory powers, all of which are discussed further below. These developments do not affect either the United Kingdom's or the Agreement's continued compliance with Section 2523(b) criteria.

A. UK General Data Protection Regulation

The United Kingdom's exit from the European Union in 2020 meant that the European Union's General Data Protection Regulation ("EU GDPR") was no longer part of United Kingdom law. However, the United Kingdom, through its Data Protection Act 2018, implemented its own General Data Protection Regulation ("UK GDPR"), which incorporates the EU GDPR directly into UK law with some modifications. The UK GDPR continues to provide a robust legal framework governing how the public and private sectors may collect, retain, use, disseminate, and otherwise process personal data in the United Kingdom. With the UK GDPR, the United Kingdom continues to provide effective oversight of the collection, retention, use, and sharing of data to satisfy requirements under 18 U.S.C. § 2523(b)(1)(B)(iv).

B. UK Online Safety Act 2023

On October 26, 2023, the UK Online Safety Act 2023 ("OSA") passed into UK law. It gives effect to the regulatory framework outlined in the Online Harms White Paper released by the UK government in April 2019 and discussed in the 2019 Explanation. The OSA introduces new criminal offenses against users of internet services sending communications containing threats, encouraging or assisting serious self-harm, cyberflashing, or consisting of abusive

intimate images.[3] The OSA also imposes new duties on providers of internet services to implement systems and processes to reduce and remove "illegal content and activity" from their platforms. This content includes: encouragement of terrorism; child sexual exploitation and abuse; controlling or coercive behavior; stalking; harassment; and promoting or facilitating suicide.[4] Moreover, the OSA imposes duties on providers to take steps against "content and activity that is harmful to children," including pornography; content that encourages, promotes, or provides instructions for self-harm, eating disorders, or suicide; bullying; and abusive and hateful content.[5]

As anticipated in the 2019 Explanation, the broad scope of the OSA may restrict freedom of expression in the United Kingdom in a manner that might not meet First Amendment protections under the U.S. Constitution if the speech took place in the United States. Despite its differences with U.S. law, however, the United Kingdom maintains protections for these freedoms as assessed in the Department of State, Bureau of Democracy, Human Rights, and Labor 2023 Country Report on Human Rights Practices in the United Kingdom[6] in a manner which demonstrates respect for freedom of speech, association, and peaceful assembly as required by 18 U.S.C. § 2523(b)(1)(B)(iii)(III).

The U.S.-UK Agreement also accounts for the essential interests of the United States to protect freedom of speech. Consistent with the CLOUD Act, Article 4(2) of the Agreement requires that orders subject to the Agreement may not be used to infringe freedom of speech. *See* 18 U.S.C.§ 2523(b)(4)(E). In further implementation of this requirement, Article 8(4) of the Agreement provides that if the United Kingdom receives data in response to an order subject to the Agreement, and the United States has declared that its essential interests may be implicated by the introduction of such data as evidence in the UK prosecution's case in a manner that raises freedom of speech concerns for the United States, then the United Kingdom must obtain permission from the United States prior to use of the data in a manner that is or could be contrary to those essential interests. In an exchange of letters conducted contemporaneously with the signature of the Agreement, the United States identified certain UK statutes that may raise freedom of speech concerns and other circumstances under which such concerns may arise, including in any situation in which UK officials have reason to believe that the offense may raise freedom of speech concerns for the United States. The United States is engaged in ongoing discussions with the United Kingdom to determine whether the offenses introduced by the OSA present freedom of speech concerns in the context of the CLOUD Act requirements. Should this be the case, the United States will supplement the list of offenses of concern specified in the exchange of letters. Consequently, the passage of the OSA does not affect either the United

[3] Online Safety Act 2023, c. 50, §§ 179-188 (UK), https://www.legislation.gov.uk/ukpga/2023/50/contents.

[4] *Id*. § 59.

[5] *Id*. §§ 60-62.

[6] U.S. Dep't of State, Bureau of Democracy, H.R. and Lab., United Kingdom 2023 Human Rights Report 2-41 (2024), https://www.state.gov/reports/2023-country-reports-on-human-rights-practices/united-kingdom/.

Kingdom's or the Agreement's continued satisfaction of requirements set forth under 18 U.S.C. § 2523(b)(4)(E).

C. Investigatory Powers (Amendment) Act 2024

On April 25, 2024, the Investigatory Powers (Amendment) Act 2024, modifying certain provisions of the Investigatory Powers Act (2016) ("IPA"), received royal assent. The IPA amendments relevant to the U.S.-UK Agreement allow for the appointment of temporary UK Judicial Commissioners providing oversight and review of targeted interception warrants and communications data authorizations issued under IPA Parts 2 and 3, respectively, and subject to the Agreement. Judicial Commissioners operate in the Investigatory Powers Commissioner's Office ("IPCO"), the entity established by the IPA to conduct independent review and oversight functions,[7] and are normally appointed by the Prime Minister for three-year, renewable terms, upon joint recommendation by a group of four senior officials that include judicial officials independent of the government. With the passage of the IPA amendments, in exceptional circumstances resulting in a shortage of Judicial Commissioners, the Investigatory Powers Commissioner may appoint temporary Judicial Commissioners for one or more terms not exceeding six months each and not exceeding three years total, and, as soon as practicable, notify the Prime Minister and the Secretary of State, among other UK officials, of the appointment.[8] This modification does not alter the effective oversight of IPA orders in satisfaction of the requirements under 18 U.S.C. § 2523(b)(1)(B)(iv).

There were additional IPA amendments that do not directly implicate 18 U.S.C. § 2523(b) criteria. Among these additional updates are an amended definition of a "telecommunications operator" and a new notification requirement for such operators, including U.S. service providers offering, providing, or controlling telecommunications services in the United Kingdom.[9] The amendments further modify obligations with respect to the review of notices under the IPA.

The definition of a telecommunications operator has been amended to clarify that large companies that operate complex corporate structures, including many major U.S. service providers with operations in the United Kingdom, are covered in their entirety under the IPA regardless of their location. Once commenced, the amendments to the IPA also allow a UK Secretary of State ("UK Secretary") to inform such telecommunications operators that they are required to notify the UK Secretary in advance of any modifications, including technical changes, to their services that could affect existing lawful access capabilities for UK authorities. Upon notification of an anticipated change to its services, a telecommunications operator may be subject to a notice, pursuant to the IPA's notices regime, requiring that the operator retain communications data, build and/or maintain technical capabilities to respond to lawful requests for data under the IPA, or take specific steps that the UK Secretary considers necessary to the interest of national security. The UK does not need to have issued an IPA order to the operator in

[7] Investigatory Powers Act 2016, c. 25, § 23 (UK), https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted.

[8] Investigatory Powers Act (Amendment) 2024, c. 9, § 9 (UK), https://www.legislation.gov.uk/ukpga/2024/9/contents.

[9] *Id.* §§ 19, 21.

advance to subject the operator to a notice. Notifications to the UK government of changes to lawful access do not automatically result in the issuance of a notice. The UK Secretary may ask the provider to submit clarifying information or choose not to act. If the UK Secretary issues a notice, the telecommunications operator has the ability to seek review of the notice. However, the IPA amendments now create a requirement that an operator not make the planned changes covered by the notice for the duration of the review period, which will now have a set time period still undergoing public consultation.

IV. Implementation of the Agreement

By regulation, the authority to perform the functions of "Designated Authority" under executive agreements authorized by the CLOUD Act is delegated to the Department of Justice's Criminal Division. In the Criminal Division, the Office of International Affairs ("OIA") serves as the U.S. Designated Authority under the Agreement and carries out its day-to-day operations, including the review, certification, and transmission of U.S. orders subject to the Agreement on behalf of U.S. federal, state, local, and territorial authorities, among other responsibilities. OIA has designed and implemented detailed procedures to execute the U.S. Designated Authority's functions, made use of technology to create a CLOUD Act case tracking system, and developed training on the Agreement and its applicable U.S. Targeting Procedures. The training was developed in coordination with the U.S. Oversight Authority under the Agreement, the Office of Intelligence ("OI") in the Department's National Security Division. The training is mandatory for U.S. users of the Agreement, who must be certified and renew the training certification every three years. To coordinate on matters of implementation of the Agreement, OIA maintains regular working level discussions with its Designated Authority counterparts at the Investigatory Powers Unit, National Directorate, Homeland Security Group, UK Home Office ("the UK Designated Authority" or "UKDA"). Moreover, OIA maintains direct communications with the United Kingdom's larger service providers covered by the Agreement and has consulted with U.S. service providers concerning the operation of the Agreement.

Pursuant to Section 2523(e)(2)(C) of the Act, OIA reports the following problems and controversies that have arisen in the course of implementation of the Agreement. None of these issues rises to the level that calls into question the determination that the United Kingdom and the Agreement continue to meet the requirements of Section 2523(b).

A. UK Prioritization of IPA Orders Has Not Provided Relief to the Mutual Legal Assistance Channel

The UKDA has reported to OIA that as of October 2024, it has transmitted 20,142 orders to U.S. service providers invoking the Agreement. Of these, 20,105 were issued pursuant to the UK's IPA,[10] the majority of which were real-time interception orders to gather intelligence relating to serious criminal activity — and thus advance the purpose of the Agreement to combat serious crime, including terrorism. Under UK law, real-time data can be used to disrupt criminal activity and for lead purposes but cannot itself be introduced as evidence in criminal

[10] The IPA is the law governing how UK government authorities, including intelligence and police services, may intercept real-time content and non-content data, among other areas.

proceedings.

In the two years the Agreement has been in force, we have not, however, seen a commensurate use of the Agreement for orders requesting evidence for criminal proceedings, and thus we have not experienced a decline in Mutual Legal Assistance Treaty ("MLAT") requests from the UK. The UKDA reports it has transmitted 37 orders pursuant to the UK's Crime (Overseas Production Orders) Act 2019 ("COPOA"), which governs law enforcement orders for stored communications and metadata that can be introduced as evidence in criminal proceedings. The UKDA has explained that there have been delays in their granting permission to UK law enforcement agencies to use the Agreement for COPOA orders. Consequently, UK authorities continue to rely on MLAT requests to seek electronic data from U.S. service providers for use in criminal investigations and prosecutions and UK MLAT requests have in fact increased slightly. Such requests continue to tax the resources of U.S. courts, federal prosecutors, investigators, and OIA, which serves as the U.S. Central Authority under MLATs as well as the U.S. Designated Authority under the Agreement.[11]

The United Kingdom made clear that its primary motivation to enter the U.S.-UK Agreement was to make use of IPA orders to combat serious crime.[12] For the United States, however, one motivation to enter the Agreement was the hope that it would lead to a decrease in the number of MLAT requests from the United Kingdom seeking electronic data stored in the United States. The Department of Justice has communicated to the UK Home Office its expectation that UK authorities will expedite the process to permit UK law enforcement agencies to transmit COPOA orders under the Agreement. In response, the UKDA has committed to reducing the number of UK MLAT requests submitted to the United States seeking electronic evidence. The UKDA reports that they have now approved some UK law enforcement agencies to use the Agreement, while others are anticipated to obtain permission with respect to a limited number of U.S. providers sometime in 2025. The UKDA also plans to coordinate with the competent UK MLAT central authority to screen UK MLAT requests to determine whether the electronic data they seek may be obtained with COPOA orders submitted under the Agreement. The Department of Justice will revisit this issue with the UKDA when assessing whether to renew the Agreement before its expiry on October 3, 2027. The Agreement also may be terminated at any time by either the United States or the United Kingdom through the exchange of diplomatic notes.[13]

While not a "problem or controversy," it should be noted that as expected the United States has made less frequent use of the Agreement than the United Kingdom. Between October 3, 2022 and October 15, 2024, the United States transmitted only 63 orders to UK providers in support of U.S. criminal investigations, all but one of which sought stored data, and most of

[11] To execute these requests, OIA and partner prosecutors must seek U.S. legal process, supported by sufficient facts to meet U.S. legal standards. UK requests often seek the content of communications but sometimes lack sufficient sourcing to meet probable cause to secure a U.S. search warrant, prompting requests for additional information from OIA. Moreover, productions involving the content of communications entail labor-intensive, filtering processes to ensure that the communications transmitted to the United Kingdom are limited to those authorized within the scope of the search warrant. By allowing UK issuing agencies to use qualifying orders to obtain electronic data directly from U.S. service providers, the Agreement was anticipated to reduce the number of UK MLAT requests submitted to the United States and thus reduce the MLAT execution burden.

[13] U.S.-UK Agreement, *supra* note 1, art. 17(2).

which resulted in production of electronic data from UK service providers. The comparatively reduced need of U.S. authorities to use the Agreement is expected to continue for the foreseeable future because the United Kingdom is not home to large providers hosting social media, email, and other online platforms of the size, number, and global scope of those located in the United States. Further, larger UK service providers principally offer telecommunications services to persons or entities located in the United Kingdom, which U.S. authorities are prohibited from targeting with orders invoking the Agreement, just as the United Kingdom is prohibited from targeting U.S. "receiving-party persons."[14]

B. UK Data Protection Challenges

While some UK service providers are complying with U.S. legal process submitted under the Agreement, lingering data protection concerns in the United Kingdom have hindered compliance by others. Data protection concerns have also slowed responses from the UKDA to U.S. requests for consent to share with third countries data obtained through the Agreement, referred to as "onward sharing" requests.[15]

Despite the UKDA's efforts encouraging UK service providers to respond to U.S. legal process[16] under the Agreement, some UK service providers remain reluctant to comply with such process, due, largely, to concerns about possible liability under the UK GDPR resulting from their compliance. The UK Information Commissioner's Office (the "ICO"), which serves as the UK's independent data protection authority, has not issued public guidance to assuage UK service providers' concerns regarding their possible liability for data transfers under the UK GDPR when responding to U.S. legal process under the Agreement. Currently, UK service providers perform a separate, case-by-case analysis of each U.S. legal process request they receive, including by making their own assessment of the legitimate interests of the U.S. investigation, as balanced against the provider's view of the specific potential prejudice to individuals whose data could be disclosed. Some UK service providers have requested additional information about: (1) the crime(s) under investigation in the matter underlying the legal process; (2) the urgency, nature, and severity of the matter under investigation; (3) the relevance and impact of the disclosure to the investigation; and/or (4) the steps taken by the

[14] The Agreement prohibits the United States and United Kingdom from targeting UK Receiving-Party Persons ("RPPs") and U.S. RPPs, respectively. *See* U.S.-UK Agreement, *supra* note 1, art. 1(12). Article 1(12) of the Agreement defines UK RPPs as (i) any governmental entity or authority of the United Kingdom; (ii) an unincorporated association, a substantial number of members of which are located in UK territory; (iii) a corporation located or registered in the United Kingdom; or (iv) any other person located in the United Kingdom. *Id.* Article 1(12) defines U.S. RPPs as (i) any governmental entity or authority of the United States, including at the state, local, territorial, or tribal level; (ii) a U.S. citizen or national; (iii) a person lawfully admitted to the United States for permanent residence; (iv) an unincorporated association a substantial number of members of which fall into subsections (ii) or (iii); (v) a corporation that is incorporated in the United States; or (vi) a person located in U.S. territory. *Id.*

[15] *See id.* art. 8(2), providing that "[an] Issuing Party shall not transfer data received pursuant to an Order subject to [the] Agreement to a third country or international organization without first obtaining the consent of the Receiving Party[.]"

[16] The Agreement defines legal process as "Orders subject to [the] Agreement as well as preservation and Subscriber Information process recognized by Article 10 of [the] Agreement." *Id.* art. 1(10).

investigation to identify the subject of the investigation. Such requests go beyond the requirements of the Agreement and are not consistent with the disclosures typically made to third parties concerning ongoing, criminal investigations. Moreover, such demands for additional information ignore the safeguards afforded to data transfers under the terms of the Agreement between the United States of America and the European Union on the Protection of Personal Information relating to the Prevention, Investigation, Detection and Prosecution of Criminal Offenses ("DPPA"), which was incorporated into the U.S.-UK Agreement. The DPPA recognizes the sufficiency of the privacy and data protection safeguards applied by the parties to that agreement – the United States and the European Union – and by extension, the United Kingdom.

While the Department of Justice understood that, under the UK GDPR, providers would need to identify a legal basis for processing data in response to each U.S. legal process, the protections and obligations set forth in the DPPA apply to the transfer of such data and its processing in the United States. The United Kingdom has not effectively communicated these safeguards to UK service providers, but has committed to addressing the issue.

The practical impact of this data protection challenge remains uncertain, largely because of the relatively small number of UK service providers that have received U.S. legal process to date. To bolster the U.S.-UK Agreement as a mechanism for cross-border data transfers, and to meet these concerns, the UK government plans to introduce amendments to the UK GDPR. The UK government's previous legislative vehicle for this amendment failed to receive approval in Parliament when a general election was called in the United Kingdom.[17] The United States understands that the United Kingdom is working to reintroduce the amendment in a new bill. The amendment would remove any doubt that the processing of data under the UK GDPR can be based on relevant international law, including specified international agreements to which the United Kingdom is a party such as this Agreement.

In addition, uncertainty about possible UK data protection requirements have slowed responses from the UKDA to U.S. requests for consent to onward sharing. The United Kingdom has delayed in specifying what information it would require in order to evaluate onward sharing consent requests in a way that is both acceptable to the United States and complies with the UKDA's perceived obligations under the UK GDPR. Consequently, while the number of requests for consent to onward sharing have been few, responses to such U.S. requests in matters involving serious, transnational, criminal activity have suffered from significant delays. The UKDA has committed to formulating and communicating the information that it will need to assess U.S. requests for consent to onward sharing.

C. U.S. Service Provider Views

In preparation for the Section 2523(e) review, OIA consulted with U.S. service providers currently complying with UK orders submitted under the U.S.-UK Agreement. OIA sought their views concerning the United Kingdom's implementation of the Agreement. Although the

[17] *See* Data Protection and Digital Information Bill (Amendment Paper), HC NC6 at 2 (Nov. 23, 2023), https://publications.parliament.uk/pa/bills/cbill/58-03/0314/amend/datapro_rm_rep_1123.pdf.

providers continue to support the Agreement and its extension through a renewal, they expressed various concerns, including concerns relating to the IPA amendments, their capacity to effectively manage increasing requirements from the United Kingdom for production in response to UK orders submitted pursuant to the Agreement, and that UK confidentiality requirements constrained their discussions with the Department of Justice.

U.S. service providers noted as a primary concern that the advance notification requirement included in the IPA amendments may lead the United Kingdom to utilize existing IPA powers to impede changes to privacy and security features that U.S. providers offer globally if such changes would affect access to data by UK authorities. Since the notification and notice regime do not involve commitments made pursuant to the Agreement or with respect to Covered Orders and do not otherwise implicate the analysis of 18 U.S.C. § 2523(b) criteria, the Department of Justice does not consider this a problem or controversy arising as a result of the Agreement or its implementation. However, DOJ has taken the opportunity of this redetermination to remind the UK of the statute's requirement that the terms of the Agreement shall not create any obligation that providers be capable of decrypting data or limitation that prevents providers from decrypting data, and the Agreement is not the only means by which the Department engages with the UK on questions of lawful access and the impact of domestic authorities on law enforcement equities.

Another major U.S. service provider expressed concerns about the production timelines of UK orders, unique data requests, and delivery requirements for the UK's increasing volume of orders. The United Kingdom transmits a significant share of UK orders under the Agreement to this provider, which OIA understands currently complies with the orders at a high rate. Although this service provider has reported to OIA that it continues to support the Agreement, the provider implied that the resources needed to address such UK orders as well as the unique requests and requirements may negatively impact the provider's responses to U.S. domestic legal process and the provider's support of the Agreement framework in the future. While providers have not raised with OIA concerns about financial reimbursement for assistance they provide under the IPA, the UKDA informed OIA that they have engaged with U.S. service providers concerning such costs.

Further, one provider said that confidentiality requirements under the IPA constrain their discussions with the Department of Justice regarding UK practices and policies. OIA requested that the United Kingdom allow the U.S. service provider to share their experiences. The UKDA advised that they had addressed the confidentiality concerns with the provider. In a subsequent conversation with that provider, OIA did not receive specific information from the provider that was relevant to the statutory considerations in the CLOUD Act enumerated at 18 U.S.C. § 2523(b).

With the continued operation of the Agreement, the Department of Justice will further engage with U.S. service providers to determine whether future UK implementation of the Agreement has improved providers' experience.

V. Conclusion

The U.S.-UK Agreement and the United Kingdom's laws and procedures continue to meet CLOUD Act requirements. The robust usage of the Agreement by UK authorities has

served as an important tool for UK efforts to combat serious crime. While the United States has had limited occasion to use the Agreement, the Agreement also has provided U.S. criminal investigations with faster access to electronic data held or controlled by UK service providers. Although the implementation of the Agreement has led to the issues reported above, the Department of Justice will continue to work with its UK counterparts to seek resolutions and will remain engaged with U.S. service providers concerning implementation and support for the Agreement.