October 29, 2019

The Honorable Lindsey Graham, Chairman
The Honorable Dianne Feinstein, Ranking Member
U.S. Senate Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Jerrold Nadler, Chairman
The Honorable Doug Collins, Ranking Member
U.S. House Committee on the Judiciary
2138 Rayburn House Office Building
Washington, DC 20515

The Honorable Jim Risch, Chairman
The Honorable Bob Menendez, Ranking Member
U.S. Senate Committee on Foreign Relations
423 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Eliot L. Engel, Chairman
The Honorable Michael McCaul, Ranking Member
U.S. House Committee on Foreign Relations
2138 Rayburn House Office Building
Washington, DC 20515

Re: U.S.-U.K. CLOUD Act Agreement

Dear Chairman Graham, Ranking Member Feinstein, Chairman Risch, Ranking Member Menendez, Chairman Nadler, Ranking Member Collins, Chairman Engel, and Ranking Member McCaul:

We write to you to about the proposed U.S.-U.K. CLOUD Act Executive Agreement, signed on October 3, 2019, which allows the transfer of personal data to foreign governments outside traditional legal process.[1] We ask you to exercise the explicit authority provided to your Committees to prevent the Agreement from entering into force.

We the undersigned privacy, civil liberties, and human rights organizations believe that the Agreement fails to adequately protect the privacy and due process rights of U.S. and U.K. citizens. We urge the House and Senate to enact a joint resolution of disapproval within 180 days. We also urge your respective Committees to use the powers granted under the CLOUD Act to seek and make public the factors relied on by the Attorney General and Secretary of State in approving the Agreement, in order to assess the full civil liberties implications of the deal.

Because the first CLOUD Act agreement will shape future deals concerning the transfer of personal data to foreign law enforcement agencies, such as the U.S.-Australia and U.S.-European Union agreements currently under negotiation, it is all the more critical that the U.S-U.K. Agreement

[1] Press Release, 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.

include robust rights protections that provide an appropriate model.[2] We believe the U.S.-U.K. Agreement falls short.

I. Background

On March 23, 2018, the Clarifying Lawful Overseas Use of Data (CLOUD) Act became U.S. law. The CLOUD Act provides for international access to stored and intercepted communications content in law enforcement investigations.[3] The Act transformed the system for cross-border access to data in criminal investigations, authorizing law enforcement in one country to directly serve requests for the production of data like email contents, or to issue a wiretap internationally, without the oversight of the nation where the interference occurs.

The CLOUD Act brought about two changes. First, U.S. authorities were newly empowered to order providers to turn over data regardless of storage location.[4] Second, the Attorney General, with the advice of the Secretary of State, was granted authority to enter into executive agreements that allow foreign authorities to request service providers to turn over stored communications contents located in the U.S. and request wiretaps in the U.S.[5] To form an executive agreement, the Attorney General, with the concurrence of the Secretary of State, must determine and submit a written certification to Congress that criteria set out in the Act have been met, including that the foreign government affords sufficient substantive and procedural protections and that the agreement includes specific safeguards.[6] An agreement lifts legal provisions which block companies' disclosure of data in response a foreign government's request. It does not create new binding legal authority to order the production of data. Any legal effect of an international request issued under an agreement must derive from the national law of the signatories.

The U.S. Congress then has 180 days to pass a joint resolution of disapproval to prevent the agreement from entering into force.[7] Your Committees are given jurisdiction over any resolution of disapproval introduced to Congress.[8] You as Committee Chair and Ranking Members are also empowered to request from agency heads a summary of the factors considered in determining that the foreign government satisfies the requirements of the Act.[9]

---

[2] 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), https://www.justice.gov/opa/pr/joint-statement-announcing-united-states-and-australian-negotiation-cloud-act-agreement-us.
[3] Consolidated Appropriations Act of 2018, Pub L 115–142, div V, §§ 101-106, 132 Stat 1213 (2018) [hereinafter CLOUD Act].
[4] CLOUD Act § 103 (codified at 18 U.S.C. §§ 2703(h), 2713).
[5] CLOUD Act § 105 (codified at 18 U.S.C. §§ 2511(2)(j), 2520(d)(3), 2702(b)(9), 2703(e)(3), 3121(a), 3124(d-e), 2523).
[6] 18 U.S.C. § 2523(b)
[7] *Id.* § 2523(d)(2).
[8] *Id.* § 2523(d)(6)(a).
[9] *Id.* § 2523(d)(3).

II. The U.S.-U.K. Executive Agreement

Since the passage of the CLOUD Act, civil society have stood in near unilateral opposition to the CLOUD Act and consistently noted the baseline protection afforded individuals under "executive agreements" fails to meet human rights standards.[10] The text of the U.S.-U.K. Executive Agreement, released by the U.K. government on October 7, 2019, exhibits many often cited concerns,[11] such as diminished standards for law enforcement requests, lack of notice, vague oversight mechanisms, and other shortcomings described below.[12]

In addition, however, we are concerned that the protections in this CLOUD Act Agreement will serve as a template for future agreements, including in cases with countries that have even more lacking data privacy standards. In such cases, additional protections embedded into an agreement itself are all the more crucial.

Diminished Standards for Access to Email Contents and Live Wiretaps

The U.S-U.K. Agreement lowers the bar for law enforcement access to both stored communications contents, such as emails, and live wiretaps in the U.S. The text of the Agreement itself eliminates the stringent probable cause requirement for foreign law enforcement access to stored content data under the Electronic Communications Privacy Act.[13] Instead, the text of the U.S.-U.K. Agreement requires that requests for content, widely considered the most sensitive electronic data, only meet the standard of "reasonable justification based on articulable and credible facts, particularity, legality, and severity."[14] This standard is vague and not clearly defined in the agreement, and likely is weaker than probable cause in various contexts. Additionally, *for the first time, it permits a foreign government to request wiretaps in the U.S. even when one of the communicants is a U.S. citizen or other person living in the U.S.* While the Agreement prohibits the U.K. from targeting U.S. persons, wiretaps can still incidentally capture their communications without having to meet the stringent intercept standard required of U.S. law enforcement, what is commonly referred to as a "super warrant" due to the heightened privacy protections provided to

---

[10] *See, e.g.*, EPIC, *The CLOUD Act*, Epic.org, https://epic.org/privacy/cloud-act/ (critiquing the act and linking articles by members of civil society).

[11] 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, U.K.-U.S., C.S. USA No. 6 (2019) (CP 178), 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 [hereinafter U.S.-U.K. Agreement].

[12] Eleni Kyriakides, *The CLOUD Act, E-Evidence, and Individual Rights*, 5 Eur. Data Protection L. Rev. 99, 102-05 (2019).

[13] 18 U.S.C. § 2703. A warrant is not required for all stored content requests under ECPA, after a federal circuit court ruling, Department of Justice (DOJ) policy is to rely on warrants to access content data. HR Rep No 114-528, 9 (2016).

[14] U.S.-U.K. Agreement art. 5(1).

wiretap targets by Congress.[15] For example, the text of the U.S.-U.K. Agreement does not independently require investigators seeking a wiretap to pursue less intrusive means, demonstrate probable cause that the facility to be wiretapped is being used in the commission of a crime, or show that the wiretap will uncover relevant evidence.[16] Additionally, the text of the Agreement does not limit requests to an initial thirty day period, or require notice to those wiretapped within 90 days, as U.S. law provides.[17] CLOUD Act agreements should instead require all requests issued meet a standard that is clearly defined and not more permissive than probable cause, and should require notice. Additionally, requests for wiretaps should be limited to a fixed duration of 30 days unless extended by a judge or magistrate.

U.K. law on the production of stored content data and live wiretaps do not raise the standards in the U.S.-U.K. Agreement and indeed at points may be weaker, emphasizing the need for strong safeguards to be written into CLOUD Act Agreements. Under the Overseas Crime Act, international orders for stored electronic data can be issued where there are "there are reasonable grounds for believing that an indictable offence has been committed" or the order relates to a terrorism investigation.[18] In addition, the Investigatory Powers Act authorizes interception warrants in various circumstances, including those targeting groups of persons. Both of these standards fall short of U.S. legal requirements for access to content and the Fourth Amendment requirements to establish individualized suspicion that a particular person is involved in the commission of a particular offense.[19] The Investigatory Powers Act authorizes interception warrants to be served on companies located outside the U.K.[20] In contrast to the rigorous and detailed limits of U.S. wiretap law, the IPA includes provisions for a renewable six month duration for interception orders (subject to further renewal) [21] and may be issued based on generalized burdens of proof that the order is necessary for "national security," "the purpose of preventing or detecting serious crime" or "in the interests of the economic well-being of the United Kingdom." [22]

Judicial Authorization Should be Requirement of the Agreement, Even if Provided for Content Orders Under U.K. Law

The text of the U.S.-U.K. Agreement itself does not require *prior* judicial authorization for requests. Instead, international requests are required to be subject to "to review or oversight" by a type of "independent authority" at some point during the lifecycle of the request – "prior to, or in

[15] 18 U.S.C §§ 2510–2522.
[16] *Id*. § 2512.
[17] *Id*.
[18] Crime (Overseas Production Orders) Act 2019, c. 5, § 4(3) (UK) [hereinafter COPO Act].
[19] *See, e.g.*, Letter From Human Rights Watch, et.al, to Justice Department Concluding White House Should Not Let U.K. Demand Private Data in U.S. (Nov. 26, 2018), https://www.hrw.org/news/2018/11/26/letter-us-justice-department-concluding-white-house-should-not-let-uk-demand-private.
[20] The Investigatory Powers Act 2016, c. 25, § 43(5) (UK) (amended 2018) [hereinafter IPA] (explaining the responsibilities with respect to an overseas recipient of an interception warrant).
[21] *Id*. § 32(2).
[22] *Id*. §§ 20, 23(1,3)

proceedings regarding, enforcement of the Order."[23] U.K. law generally provides for prior judicial review of law enforcement orders *for content*.[24] However, this review appears less rigorous than the level of judicial review required under the Fourth Amendment.[25] Thus, as a result, requests to U.S. providers to produce or intercept content may in practice be subject to reduced independent judicial review as compared with the warrant or Wiretap Act process. Against this domestic backdrop, the requirement for prior judicial authorization could simply have been incorporated into the text of the U.S.-U.K. Agreement and, yet, was not. Future agreements which apply this language from the U.S.-U.K. Agreement may not have the benefit of backstop domestic requirements for judicial approval. Domestic regimes are also subject to change; an express requirement for judicial authorization in the U.S.-U.K. Agreement would ensure consistent protection. Prior judicial authorization of law enforcement orders provides the best guarantee of procedural fairness, and, particularly for access to sensitive data, is the default rule.[26] Prior judicial authorization prevents flawed orders from moving forward before data is accessed and the damage is done. For this reason, approval by a neutral magistrate is a cornerstone of the constitutional warrant requirement and mandatory for U.S. domestic orders for stored content and intercepts.[27] Prior judicial authorization should be a requirement under all CLOUD Act agreements.

Unequal Minimization and Targeting Protections for U.K. and U.S. Citizens

Under the U.S.-U.K. Agreement, requirements for minimization of data and targeting individual requests do not apply equally to the U.S. and U.K. Requirements to minimize data only benefit U.S. persons. The Agreement requires the U.K. to adopt procedures to minimize the acquisition, retention, and dissemination of information concerning U.S. persons acquired under the Agreement.[28] However, no minimization procedures are required of the U.S. for U.K. persons' data. These minimization procedures should apply equally to U.S. and U.K. persons. Procedures for targeting individual requests under the agreement are also one sided.[29] As a member of the EU, the UK may not discriminate between its own citizens and those of other member states; it could not include targeting limitation applicable to UK citizens. As a result, the Agreement permits the U.S. to

[23] U.S.-U.K. Agreement art. 5(2).
[24] IPA, *supra* note 21, § 23; COPO Act, *supra* note 19, § 1(1).
[25] *See, e.g.*, Mailyn Fidler & Scarlet Kim, *In the U.S.-U.K. Deal, Both Sides Deserve Scrutiny*, Just Security (August 9, 2017), https://www.justsecurity.org/44020/u-s-u-k-deal-sides-deserve-scrutiny1/.
[26] *See, e.g.*, *Szabó*, App. No. 37138/14, Eur. Ct. H.R., Judgment, 40 (2016).
[27] U.S. Const. amend. IV.
[28] U.S.-U.K. Agreement art. 7(2-5).
[29] United Kingdom, 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 3 (2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836970/EM_CS_USA_6.2019_UK_USA_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.odt.

target U.K. citizens located outside the U.K, while the U.K. is barred from targeting U.S. citizens and residents using requests issued under the Agreement.[30]

No Notice to the Data Subject nor Remedies

The U.S.-U.K. Agreement does not require notice be provided to the data subject. Notice is essential to the ability to access remedies: without notice, an individual will not be aware that surveillance occurred, may not be able to pursue remedies if appropriate, may raise obstacles to demonstrating standing in court, and may not be able to adequately interrogate the evidence against them.[31] Additionally, the U.S.-U.K. Executive Agreement explicitly forestalls the possibility that the deal would provide any new remedy to individuals.[32] Effective remedies are considered essential under countless human rights instruments.[33] At a minimum, U.S. and U.K. domestic remedies and opportunities to challenge requests reasonably available to individuals whose data are accessed under the Agreement should be clarified in an annex to the Agreement.

Low Threshold for Covered Crimes

While the U.S.-U.K. Agreement has been heralded by the DOJ for targeting crimes of "terrorism, sexual abuse, and cybercrime," the offenses for which requests may be issued are not so limited.[34] The Agreement permits international requests for *all* offenses punishable by a prison term of a maximum term of at least three years.[35] A recent report commissioned by the European Parliament found that an equivalent limitation proposed in EU law failed to exclude petty crimes,

---

[30] *Id*. Each party is required to adopt targeting procedures designed to ensure orders target an account of a "Covered Person," who can be anyone besides a "Receiving-Party Person." U.S.-U.K. Agreement art 1(6), 7(1). The U.K. may not target "(i) any governmental entity or authority [of the United States], including at the state, local, territorial, or tribal level; (ii) a citizen or national thereof; (iii) a person lawfully admitted 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 its territory." *Id*. art. 1(12). The U.S. is permitted to target U.K. citizens and permanent residents. The U.S. is only barred from targeting: "(i) any governmental entity or authority of the [U.K.]; (ii) an unincorporated association, a substantial number of members of which are located in its territory; (iii) a corporation located or registered in its territory; or (iv) any other person located in its territory." *Id*. art. 1(12).

[31] *See, e.g.*, *Big Brother Watch and Others v. United Kingdom*, Nos. 58170/13, 62322/14 and 24960/15, § 310, ECHR 2018.

[32] *Id*. art. 3(4).

[33] International Covenant on Civil and Political Rights, Dec. 16, 1966, S. Exec. Doc. E, 95-2 (1978), 999 U.N.T.S. 171 (entered into force Mar. 23, 1976); European Convention on Human Rights art. 13, Nov. 4, 1950, ETS No. 005; Charter of Fundamental Rights of the European Union, art. 47, Dec. 18, 2000, 2000 O.J., 1, 10 (C 83) (entered into force Dec. 1, 2009).

[34] Press Release, U.S. And UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online, *supra* note 1.

[35] U.S.-U.K. Agreement art. 1(5,14).

sweeping in crimes such as simple theft, fraud, and assault.[36] "[A] requirement that will be met by most offences under national law, cannot be considered an adequate threshold for particularly intrusive measures," the report concluded.[37] Yet under the U.K. Investigatory Powers Act access to content of a communication, either in transit or stored, is limited to "serious offenses," defined as either an offense where an adult without previous convictions could reasonably be expected to be sentenced to a *minimum* of three years imprisonment, or an offense involving specified conduct.[38] It is not clear why the Agreement, which defines serious crime based on a sentence with a *maximum* punishment of three years in prison, could not have imported the higher bar available in U.K. law.

Additionally, conduct may also be criminal in one jurisdiction yet not an offense in a second, or punished more heavily in one nation over the other. A three-year prison term threshold should be supplemented with more stringent requirements, including a requirement for dual criminality.[39] The requirement of dual criminality, "that the offense for which the foreign state seeks assistance also constitutes a crime in the requested state," is a cornerstone of extradition treaties that help prevent political or unjust prosecutions, and which support reciprocity between states.[40] While not typically included in the text of MLAT agreements, U.S. law already requires dual criminality by statute: 18 U.S.C. § 3512(e) provides that an ECPA warrant can be issued based on a foreign government's request for assistance only when the conduct being investigated would be a felony in the U.S.[41] Applying the principle of dual criminality in this new context is only more important given that many of the MLAT's oversight safeguards are removed from the Executive Agreement.[42] Dual criminality is therefore a necessary requirement for Executive Agreements undertaken pursuant to the CLOUD Act.

Vague External Oversight

While some external oversight is built into the U.S.-U.K. Agreement, the safeguards lack sufficient detail to ensure rigorous review. For example, a joint review of the Agreement is required after one year, but only a "periodic" review thereafter.[43] The content of the original and following periodic review is only defined generally as a "review of the issuance and transmission of Orders"

---

[36] Policy Dep't for Citizens' Rights & Constitutional Affairs, Eur. Parliament, An Assessment of the Commission's Proposals on Electronic Evidence 40 (2018), https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604989/IPOL_STU(2018)604989_EN.pdf.

[37] *Id*.

[38] IPA, *supra* note 21, § 263(1) (UK).

[39] *See, e.g.*, Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, O.J. L 130/1 (requiring dual criminality for Europe wide investigation orders).

[40] T. Markus Funk, Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges 11 (2014), https://www.fjc.gov/sites/default/files/2017/MLAT-LR-Guide-Funk-FJC-2014.pdf

[41] 18 U.S.C. § 3512(e)

[42] *See, e.g.*, Eur. Data Protection Bd., Opinion 23/2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters (Art. 70.1.b) 6 (2018), https://edpb.europa.eu/sites/edpb/files/files/file1/eevidence_opinion_final_en.pdf.

[43] U.S.-U.K. Agreement art. 1(5,14).

and "handling of data acquired."[44] This text does not define how often subsequent reviews must occur, whether the fact of or the results of the review will be made public, if a public consultation will be conducted, the criteria for review, or any concrete output like a report. Contrast the opacity of the surveillance authority established under the U.S.-U.K. Executive Agreements with the very detailed public reporting requirements contained in the U.S. federal wiretap law.[45] This reporting requirement includes an overview of the cost, duration, and effectiveness of wiretap surveillance annually in the U.S. and records of deeper statistical measures like the type of crimes for which wiretaps were issued.[46] Under U.S. law, judges which issue wiretap orders must annually report: the fact of an application for an order or extension, the type of order or extension applied for, whether the order or extension was granted, modified, or denied, the period of interceptions authorized including whether there were any extensions, the underlying offense, the identities of the law enforcement applicant and the person authorizing the application, and the nature of the facilities where the intercept occurred.[47] These reports are consolidated and made public, providing insight as to the cost and effectiveness of electronic surveillance techniques.[48]

Under the Agreement, each country's authority granted oversight over these international requests is required annually report certain aggregate statistical data.[49] However, without giving content to the reporting requirement and explicitly requiring a compliance audit, it is difficult to assess whether the statistical data provided will serve as any public check, or even provide useful information to oversight authorities and researchers. To define a successful reporting regime, the Agreement could have imported the requirements of the annual U.S. Wiretap Reports.

Weak Human Rights Protections and Free Expression Concerns

A critical human rights protection in the Mutual Legal Assistance Treaty (MLAT) process is a requirement that a U.S. entity, namely the DOJ and a judge, review a foreign request for content to ensure that it does not raise human rights concerns. Such a protection is critical because even generally rights-respecting jurisdictions may have particular laws or practices that raise human rights concerns. The U.S.-U.K. Agreement jettisons this important protection by permitting providers to respond directly to requests from the U.K. Under the agreement, the U.S. does not even perform a cursory review of such requests, requests that are potentially contrary to U.S. interests or human rights. In addition, under the Agreement, the U.K. government need not even inform the U.S. an request has been issued in all circumstances. This essentially leaves providers as the last line of

[44] *Id*.
[45] 18 U.S.C. § 2519 ("Reports concerning intercepted wire, oral, or electronic communications").
[46] *Id*.
[47] 18 U.S.C. § 2518(1).
[48] *See, e.g.*, United States Courts, *Wiretap Reports 2018*, Uscourts.gov (Dec. 31, 2018), https://www.uscourts.gov/statistics-reports/wiretap-report-2018. *See also* Testimony and Statement for the Record of Marc Rotenberg, Executive Director, EPIC, Hearing on "The FISA Amendments Act of 2008," Before the House Committee on the Judiciary Subcommittee on Crime, Terrorism, and Homeland Security (May 12, 2012) ("Such information is critical to evaluating both the effectiveness and the need for various types of Government surveillance activities."), https://epic.org/privacy/testimony/EPIC-FISA-Amd-Act-Testimony-HJC.pdf.
[49] U.S.-U.K. Agreement art. 15(4).

defense and does not reflect the reality that many providers will not have the capacity or interest in conducting robust human rights reviews of requests received.

In addition, the agreement fails to fully comply with provisions in the CLOUD Act that stipulate that an request issued by a foreign government may not be used to "infringe freedom of speech." Under the agreement, the U.K. is not permitted to use information in cases where "the United States has declared that its essential interests may be implicated by the introduction of such data as evidence in the prosecution's case in the United Kingdom in a manner that raises freedom of speech concerns for the United States." This fails to meet CLOUD Act standards. The provision relates only to the introduction of information as evidence, which does not cover the scope of actions that may infringe on free speech. Merely gathering evidence, without use in subsequent prosecutions, may raise free speech concerns.

Circumvention of the Fourth Amendment

The Agreement also permits the U.K. to share information with the U.S. government about Americans, collected under standards that fall short of the Fourth Amendment, provided the information relates "to significant harm, or the threat thereof, to the United States or U.S. persons."[50] Under the Agreement, this could include even information about "significant financial fraud", where there is no imminent threat to life and safety.[51] This loophole should be narrowed to only permit sharing of information where there is an imminent threat to life and safety, and the U.S. government should be required to publicly report how often information is received pursuant to this provision.

Procedural Issues

At the time of the signature of this Agreement, the U.K. is a member of the European Union, raising questions regarding the ability of a single EU member state to enter into a bilateral Agreement with the U.S. without violating EU law. Members of the European Parliament wrote to the EU Commission about this matter and related concerns, and are awaiting a response.[52]

III. Conclusion

We urge you as Committee leaders to exercise your statutory powers of request for information underlying the U.S.-U.K. Agreement, to publicly release that information, and to pursue a resolution of disapproval. Thank you for your timely attention to this pressing issue. We look forward to working with the Committees to ensure appropriate civil liberties and due process protections in cross-border law enforcement access to data.

Please feel free to EPIC International Counsel Eleni Kyriakides regarding this statement at kyriakides@epic.org.

[50] U.S.-U.K. Agreement art. 7(5)
[51] *Id*.
[52] @moritzkoerner, Twitter (Oct. 7, 2019 8:20 AM), https://twitter.com/moritzkoerner/status/1181227915738042370 (including the MEP letter).

Sincerely,

Access Now
American-Arab Anti-Discrimination Committee (ADC)
Constitutional Alliance
Consumer Action
Defending Rights & Dissent
European Digital Rights (EDRi)
Electronic Frontier Finland
Electronic Frontier Foundation
Electronic Privacy Information Center (EPIC)
Government Accountability Project
Homo Digitalis
Human Rights Watch
Initiative für Netzfreiheit
Liberty Coalition
Open Rights Group
New America's Open Technology Institute
Restore The Fourth
Statewatch
TechFreedom
Vrijschrift

cc: The Honorable Mitch McConnell, Senate Majority Leader
The Honorable Chuck Schumer, Senate Minority Leader
The Honorable Steny Hoyer, House Majority Leader
The Honorable Kevin McCarthy, House Minority Leader