HIDING IN THE EYE OF THE STORM CLOUD: HOW CLOUD ACT AGREEMENTS EXPAND U.S. EXTRATERRITORIAL INVESTIGATORY POWERS

TIM COCHRANE*

The United States and United Kingdom will soon implement a new reciprocal international law enforcement data sharing agreement (U.S.-UK Agreement), the first of its kind under the Clarifying Lawful Overseas Use of Data Act 2018 (CLOUD Act), which will enable law enforcement of one signatory state to directly request data from service providers based in the other state. The United States says CLOUD Act agreements simply remove conflicts of law and do not affect its jurisdiction over overseas providers, claiming these are strictly constrained by the personal jurisdiction requirement contained within the Constitution's Fifth Amendment Due Process Clause. It is widely believed that that the United States will issue few, if any, U.S.-UK Agreement requests.

This article critiques this belief, examining the impact of CLOUD Act agreements at public and private international law, as well as domestic U.S. and UK law. While the removal of conflicts is a significant private international law benefit itself, CLOUD Act agreements also allow signatory states to significantly expand enforcement jurisdiction over overseas providers at public international law. Under domestic U.S. law, such expanded jurisdiction does not appear to be meaningfully constrained by the Due Process Clause, nor would new legislation necessarily be required. Frequent United States use of CLOUD Act agreements should be presumed.

* Ph.D. candidate, University of Cambridge Faculty of Law; M.Phil. Law (Dist.), University of Oxford Faculty of Law; LL.M. (Dist.), University of Pennsylvania Law School; LL.B./B.A. (Hons.), University of Otago; Attorney and Counselor-at-Law, New York State; Solicitor, Senior Courts of England and Wales; Barrister and Solicitor, High Court of New Zealand (all currently non-practising). This article, which was last substantially updated in September 2021, was drafted while the author was in receipt of the Fitzwilliam College Stan Gold PhD Studentship. The author would like to thank Oliver Butler, David Erdos, Asaf Lubin, David Matyas, Jessica Shurson, and Kaiyi Xie for comments, as well the journal staff for their very helpful feedback. The usual disclaimers apply.

I. INTRODUCTION: DIRECT ACCESS MECHANISMS IN OUR DIGITAL WORLD

A new generation of international "direct access" mechanisms offers states previously unparalleled opportunities to extend their law enforcement investigatory data gathering powers extraterritorially to more quickly obtain data from service providers that are operating in other jurisdictions. The most

advanced of these mechanisms, and the focus of this article, are bilateral "CLOUD Act" agreements, promoted by the United States and issued under its 2018 Clarifying Lawful Overseas Use of Data Act (CLOUD Act).[1] The first, and so far only, CLOUD Act agreement was signed between the United States and United Kingdom in 2019 (U.S.-UK Agreement), and is expected to come into force imminently as of the time of writing.[2] While such agreements are reciprocal—allowing both sovereign states equal use of their provisions[3]—it is widely believed that the United States will have little to no incentive to directly use CLOUD Act Agreements to request data from overseas.[4] This article critiques this belief. It outlines the international law benefits of CLOUD Act agreements and other direct access mechanisms and argues that the United States should be considered motivated and capable to make robust use of CLOUD Act agreements. Just as the U.S.-UK Agreement will speed up UK law enforcement's access to data from U.S. service providers like Google, Facebook, and Twitter,[5] it may equally facilitate access by U.S. law enforcement to that same data, as well as well as equivalent data from UK providers, such as BT, Virgin Media O2, and Icedrive.[6]

---

1. Clarifying Lawful Overseas Use of Data (CLOUD) Act, Pub. L. No. 115–141, 132 Stat. 1213 (2018) (codified in scattered sections of 18 U.S.C.).

2. Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime, UK-U.S., Oct. 3, 2019 [hereinafter U.S.-UK AGREEMENT]; *see* HOME OFF., IA NO. HO0383, IMPACT ASSESSMENT: POLICE, CRIME, SENTENCING AND COURTS BILL 7 (2021) (UK) (noting, as of June 30, 2021, "the [U.S.-UK Agreement] . . . is expected to come into force in 2021."). For reasons for this delay, see *infra* note 144.

3. CLOUD Act § 105, 18 U.S.C. §2523(b)(4)(I) (2018) (requiring that foreign states party to executive agreements "afford reciprocal rights of data access"); *e.g.*, U.S.-UK AGREEMENT, *supra* note 2, art. 2(3)(b) (referencing "the spirit of reciprocity in international cooperation"); *see* Press Release, U.S. Dep't of Just., Off. Pub. Affs., 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 [hereinafter Data Access Agreement Press Release]; Sujit Raman, Assoc. Deputy Att'y Gen., U.S. Dep't Just., Remarks to the Center for Strategic and International Studies (May 24, 2018), https:// www.justice.gov/opa/ speech/ associate-deputy-attorney-general-sujit-raman-delivers-remarks-center-strategic-and.

4. *See infra* Part 0.C.

5. *See, e.g.*, HC Deb (1 Dec. 2018) (650) col. 594 (UK) (recognizing this).

6. BT describes itself as "a leading communications service provider selling products and services to consumers, small and medium sized enterprises and the public sector." *Our Company*, BT, https:// www.bt.com/ about/bt/our-company (last visited Sept. 5, 2021). Virgin Media O2 is a recently formed amalgamation of two service providers, "combining the UK's largest and most reliable mobile network with a broadband network . . . ." *Hello, We're Virgin Media O2*, VIRGIN MEDIA O2, https:// news. virginmediao2.co.uk/about-us (last visited Sept. 5, 2021). Similarly, Icedrive provides "[t]he next generation of cloud storage," ICEDRIVE, https://icedrive.net/ (last visited Sept. 5, 2021), and is "controlled and offered . . . from . . . facilities in the United Kingdom." *Terms of Service*, ICEDRIVE, https:// icedrive. net/ (last visited Sept. 5, 2021). For a detailed list of UK service providers, at least some of which have no U.S. operations whatsoever, see *Members*, ISPAUK, https:// www.ispa. org.uk/members/ (last visited

This article proceeds in four parts. Part II provides background context, outlining the CLOUD Act and the U.S.-UK Agreement and its reception. Its analysis, both in Part II and throughout, focuses on the possibility for CLOUD Act agreements to be used to facilitate access to stored data through requests under the U.S. Stored Communications Act (SCA)—and it assumes these requests would be filed by federal law enforcement in federal courts.[7] Part III critiques the belief that the United States has little to no incentive to seek to directly use CLOUD Act agreements to obtain extraterritorial data.[8] It responds to the primary United States' guidance on the CLOUD Act and agreements made under it, set out in an April 2019 U.S. Department of Justice (DOJ) white paper (*White Paper*).[9] The *White Paper* argues that CLOUD Act agreements "only remove potential conflicts of law" and do not "allow the U.S. government to acquire data that it could not before."[10] Whether U.S. law enforcement may assert jurisdiction over foreign service providers continues to be based on unchanged constraints under the U.S. Constitution, the *White Paper* states—referring to the "personal jurisdiction" requirement of the Due Process Clause within the Fifth Amendment.[11]

Responding to this, Part III explains why the United States will be *motivated* to channel requests for extraterritorial data through CLOUD Act agreements. It does so by considering the benefits of CLOUD Act agreements and similar direct access mechanisms at international law. Extrapolating from the United Kingdom's implementation of the U.S.-UK

Sept. 5, 2021).

7. *See, e.g.*, Robert J. Peters et al., *Not an Ocean Away, Only a Moment Away: A Prosecutor's Primer for Obtaining Remotely Stored Data*, 47 MITCHELL HAMLINE L. REV. 1072, 1094, 1098 (2021) (similarly assuming that CLOUD Act agreement requests would be made through these and analogous statutes). While state law enforcement may also seek these orders, federal requests appear to be far more common. *See* Stored Communications Act, 18 U.S.C. §§ 2703, 2711(4) (as amended following the CLOUD Act) [hereinafter SCA] (permitting SCA requests to be filed by both state and federal officials and heard in both state and federal courts). *See generally* U.S. DEP'T OF JUST., SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS (2009), https:// www. justice.gov/ sites/ default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf (summarizing SCA case law, which predominantly involves federal law enforcement in federal courts).

8. *See infra* Part II.C.

9. 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 10 (2019) [hereinafter U.S. WHITE PAPER].

10. *Id.* at 4, 13.

11. *Id.* at 8, 14; *see In re* Grand Jury Investigation of Possible Violations of 18 U.S.C. § 1956 & 50 U.S.C. § 1705, 381 F. Supp. 3d 37, 50 (D.D.C. 2019), *aff'd sub nom In re* Sealed Case, 932 F.3d 915 (D.C. Cir. 2019). *See generally* U.S. CONST. amend. V ("No person shall . . . be deprived of life, liberty, or property, without due process of law"). The Fourteenth Amendment, which applies to state conduct, is in similar terms. U.S. CONST. amend. XIV ("No State shall . . . deprive any person of liberty, liberty, or property, without due process of law"). Federal SCA requests engage the Fifth Amendment. *See infra* note 248.

Agreement, it explains that these mechanisms appear to provide benefits at both private and international law. First, countries are increasingly enacting "blocking laws," asserting limitations on the ability of foreign states to access data processed by providers within their jurisdiction. These blocking laws create conflicts of law. A private international law benefit of CLOUD Act agreements is that they provide a remedy for these conflicts, albeit a partial one.[12] Absent a negotiated resolution between the United States and European Union (EU), bilateral direct access arrangements may be unable to resolve the conflicts presented by the blocking statute that U.S. law enforcement perhaps fear most: the EU General Data Protection Regulation (GDPR).[13] Second, law enforcement also frequently face delays in obtaining data from providers and others beyond their jurisdiction,[14] as this commonly requires using international processes like mutual legal assistance (MLA), which may take months or years.[15] However, as the United Kingdom's own approach to the U.S.-UK Agreement indicates, a public international law benefit of CLOUD Act agreements is that they permit their members to positively expand jurisdiction over service providers previously beyond their (jurisdictional) reach, allowing swift access to such data as compared to the MLA process. Recent U.S. law enforcement experience indicates they will be motivated to seek both these benefits—if doing so is permissible under U.S. domestic law.

Having addressed the United States' motivation in Part III, Part IV considers its *capability* to benefit from CLOUD Act agreements as a matter of U.S. law. While the motivation of U.S. law enforcement to use such agreements to minimize conflicts of law (the private international law benefit of these agreements) is debated, its lawful ability to do so is not in doubt.[16] Part IV therefore focuses on the lawful ability of U.S. law enforcement to use the second benefit of CLOUD Act agreements: asserting jurisdiction over foreign service providers previously outside their scope (the public international law benefit). The primary argument that this second benefit is

12. *See infra* Part III.A.

13. Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR]; *see also infra* note 137 (outlining a related EU law instrument and explaining why this article focuses on the GDPR).

14. *See infra* Part II.A.

15. *See infra* Part 0.A. Other processes that may be available, such as letters rogatory, may be even slower. *See, e.g.*, T. Markus Funk, *The Key Tools of the Trade in Transnational Bribery Investigations and Prosecutions: Mutual Legal Assistance Treaties (MLATs) and Letters Rogatory*, *in* FROM BAKSHEESH TO BRIBERY: UNDERSTANDING THE GLOBAL FIGHT AGAINST CORRUPTION AND GRAFT 547, 551 (T. Markus Funk & Andrew S. Bourtors eds., 2019).

16. *See infra* Part III.A.

unavailable, set out in the *White Paper*, derives from the U.S. Constitution's Fifth Amendment Due Process Clause. This typically requires U.S. courts be satisfied that foreign persons have sufficient "minimum contacts" with the United States that the exercise of "personal jurisdiction" over them would be reasonable.[17] It is, however, seriously questionable whether the Due Process Clause imposes any meaningful restrictions in this context.[18] Further, whether these constitutional restraints protect such foreign service providers at all is far from clear.[19] This part also critiques related arguments that the ability of U.S. law enforcement to exercise such expanded jurisdiction is merely theoretical.[20] Ultimately, U.S. law enforcement is not bound by the *White Paper*'s interpretation and, moreover, may be able to expand jurisdiction over foreign service providers without any additional legislative amendments whatsoever.[21]

This article's main audience is foreign states considering CLOUD Act agreements or similar international direct access arrangements. It may also inform service providers and others seeking to understand the U.S.-UK Agreement, as well as courts faced with likely jurisdictional challenges to its use.[22] This article hopes to provide two contributions. First, its analysis of the international law implications of direct access mechanisms seeks to contribute to ongoing discussions about the merits of these new mechanisms generally. Direct access mechanisms are not only a United States phenomenon; the UK legislation enabling the U.S.-UK Agreement envisages separate bilateral agreements with foreign states,[23] and analogous new Australian legislation is even broader, permitting "multilateral" arrangements.[24] Perhaps most significant are ongoing discussions about

17. *See infra* notes 76–84.

18. *See infra* Part IV.A(1).

19. *See infra* Part IV.A(2).

20. *See infra* notes 89–90.

21. *See infra* Part IV.B.

22. William Schwartz, Andrew Goldstein & Daniel Grooms, *How the CLOUD Act is Likely to Trigger Legal Challenges*, N.Y.L.J. (Mar. 31, 2020), https:// cdp.cooley. com/wp-content/uploads/ 2020/ 04/NYLJ03302020444632Cooley.pdf ("Production orders issued under the Agreement are almost certain to trigger legal challenges on both sides of the Atlantic that will raise novel issues of domestic and international law."); Rebecca Niblock, *On Its Way: The UK-US Bilateral Data Access Agreement*, KINGSLEY NAPLEY: CRIM. L. BLOG (June 19, 2020), https://www.kingsleynapley.co.uk/insights/blogs/ criminal-law-blog/on-its-way-the-uk-us-bilateral-data-access-agreement#page=1 ("Once [COPOA is] in force, the inevitable teething difficulties with interpretation and legal challenges are likely to lead to initial delay . . . .").

23. Crime (Overseas Production Orders) Act (COPOA) 2019, c. 5, §§ 1, 4 (UK); *see* HOME OFF., IA NO. HO0315, IMPACT ASSESSMENT: CRIME (OVERSEAS PRODUCTION ORDERS) BILL 3 (2018) (UK) ("The legislation may enable wider data sharing agreements with other foreign countries leading to an improvement of international relations and information sharing to combat serious crime.").

24. *Telecommunications Legislation Amendment (International Production Orders) Act 2021* (Cth)

similar direct access mechanisms within the EU and between the State Parties to the "Budapest" Cybercrime Convention,[25] administered by the Council of Europe (CoE).[26] The data these mechanisms seek to facilitate access to are widely viewed by these countries and bodies as "critical" for "investigations of serious crime" in today's digital world.[27]

This article's second contribution arises from its focus on the United States. As the current home of the bulk of the world's leading service providers,[28] the United States is predicted to become the center of a "hub-and-spoke" model of direct access mechanisms.[29] Australia is already negotiating a CLOUD Act agreement with the United States, and New Zealand appears similarly motivated to take this step.[30] Related EU-U.S.

---

sch 1 pt 1 s 3 (Austl.).

25. *Proposal for a Regulation for the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters*, COM (2018) 225 final (Apr. 17, 2018) [hereinafter *European Commission Proposal*]; Council of Europe, Cybercrime Convention Committee*, Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence,* CM(2021)57-final (Nov. 17, 2021) [hereinafter *Second Additional Protocol*]. *See generally* Computer Crime Convention Between the United States of America and Other Governments, Nov. 23, 2001, T.I.A.S. 13174, E.T.S. 185 [Budapest Convention].

26. *See The Council of Europe and the European Union: Different Roles, Shared Values*, COUNCIL OF EUR., https:// www.coe.int/ en/web/portal/european-union (last visited Feb. 1, 2021) (stating all EU member states are also members of the Budapest Convention, although Budapest Convention membership extends more broadly around the globe to include Canada, Japan, South Africa, and others).

27. *See* U.S. WHITE PAPER, *supra* note 9, at 2; HOME OFF., 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 ¶ 1 (2019) (UK) [hereinafter UK EXPLANATORY MEMORANDUM] (referring to such data as "a vital source of evidence for the investigation and prosecution of serious crimes"); *European Commission Proposal*, *supra* note 25, at 1 (suggesting that EU member state law enforcement "require access to data" overseas "in a growing number of criminal cases"); *Second Additional Protocol, supra* note 25, at 4 (similarly noting "evidence of any criminal offence is increasingly stored in electronic form on computer systems in foreign, multiple or unknown jurisdictions"); Commonwealth, *Parliamentary Debates*, House of Representatives, 5 March 2020, 2647 (Alan Tudge, Member of Parliament) (Austl.) ("Crucial electronic evidence—from messages between violent extremists plotting terrorist attacks, drug syndicates planning major imports to child exploitation material shared on online platforms—is often stored out of Australian agencies' reach.").

28. *See* U.S. WHITE PAPER, *supra* note 9, at 2.

29. Bertrand de la Chapelle, *Territoriality and the Cross-Border Internet: Three Exemplary Challenges*, *in* HUMAN RIGHTS CHALLENGES IN THE DIGITAL AGE: JUDICIAL PERSPECTIVES 123–25 (2020).

30. *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*, U.S. DEP'T. OF JUST. (Oct. 7, 2019), https://www.justice.gov/opa/pr/joint-statement-announcing-united-states-and -australian-negotiation-cloud-act-agreement-us; *see* N.Z. GOVERNMENT, CYBER SECURITY, WHY IS NZ CONSIDERING JOINING THE BUDAPEST CONVENTION? 2–3 (2020), https:// consultations. justice. govt.nz/policy/budapest-convention/user_uploads/2.-why-is-nz-considering-joining-the-budapest-convention.pdf (referring to New Zealand possibly signing a CLOUD Act agreement with the United States).

negotiations are ongoing.[31] Other jurisdictions, such as Switzerland, are also evaluating the potential of CLOUD Act agreements.[32] This article may be of interest to all countries and regions seeking to understand the benefits and risks of CLOUD Act agreements—or, indeed, any similarly structured direct access mechanism. Ultimately, if nations wish to move forward with such agreements they should do so with the full knowledge that these agreements are reciprocal and on the assumption that the United States, as well as any other foreign counterparts, may well make frequent use of them to directly compel data from service providers based in counterpart states.

II. CLOUD ACT EXECUTIVE AGREEMENTS AND RECEPTION TO DATE

This Part first outlines the CLOUD Act, explaining its impetus and effect. It then discusses the U.S.-UK Agreement. Finally, it elaborates the conventional wisdom, driven by the United States' repeated comments, that U.S. law enforcement have little motivation to seek data using CLOUD Act agreements and, indeed, limited ability to do so as a matter of U.S. law in any event.

A. The CLOUD Act

This discussion begins with the CLOUD Act, described by its Senate sponsor "as a tremendously important bill that will help to solve the problems that have arisen in recent years with cross-border law enforcement requests."[33] This legislation, enacted in March 2018, "accomplished two things."[34] First—the focus of most commentary—it added 18 U.S.C. § 2713

31. *Joint US-EU Statement on Electronic Evidence Sharing Negotiations*, U.S. DEPT. OF JUST. (Sept. 26, 2019), https:// www. justice.gov/opa/ pr/ joint- us- eu-statement- electronic-evidence-sharing-negotiations. *See generally* Theodore Christakis & Fabien Terpan, *EU-US Negotiations on Law Enforcement Access to Data: Divergences, Challenges and EU Law Procedures and Options*, 11 INT'L DATA PRIV. L. 81 (2021) (providing "the context of these [EU-US] negotiations and the numerous challenges surrounding them").

32. DÉPARTEMENT FÉDÉRAL DE JUSTICE ET POLICE [FEDERAL DEPARTMENT OF JUSTICE AND POLICE], RAPPOT SUR LE US CLOUD ACT (LOI *CLOUD*) (SEP. 17, 2021) [REPORT ON THE U.S. CLOUD ACT (CLOUD LAW)] (2021) (Switz.); *see, e.g.*, Dep't of Public Safety and Emergency Preparedness Canada, *CLOUD Act*, GOV'T OF CAN. (Nov. 20, 2019), https://www.publicsafety.gc.ca/cnt/trnsprnc/ brfng- mtrls/trnstn-bndrs/20191120/034/index-en.aspx (briefing the incoming minister on the CLOUD Act, and noting that certain Canadian law enforcement have "expressed support for Canada entering negotiating with the [U.S.] with the aim of concluding a CLOUD Act agreement," but redacting proposed next steps).

33. 164 Cong. Rec. S596 (daily ed. Feb. 5, 2018) (statement of Sen. Orrin Hatch). I provide a more detailed description of the background to the CLOUD Act and U.S.-UK Agreement elsewhere. Tim Cochrane, *Digital Privacy Rights and CLOUD Act Agreements*, 47 BROOK. INT'L. L.J. (forthcoming 2022) (manuscript at 7–24) (on file with author).

34. Richard W. Downing, Deputy Assistant Att'y Gen., U.S. Dep't of Just., Delivering Remarks at

to the SCA.[35] The SCA "creates a set of Fourth Amendment-like privacy protections by statute" for stored data held by U.S. service providers.[36] It limits the bases by which such providers may voluntarily disclose user data and regulates the methods by which the U.S. government may compel disclosure.[37] The SCA's new § 2713 now requires service providers subject to U.S. jurisdiction to disclose data pursuant to SCA requests "within such provider's possession, custody, or control, regardless of" the data's location.[38] This addition famously mooted the then pending U.S. Supreme Court *Microsoft Ireland* litigation.[39] Whether § 2713 simply "restor[ed] the widely accepted and long-standing understanding of U.S. law," as the United States claims,[40] or actively expanded the SCA's reach extraterritorially, is debated.[41] In any event, § 2713 confirmed Congress' intention to provide the SCA broad extraterritorial scope over data.[42]

As its second accomplishment—and the focus of this article—the CLOUD Act allows the United States to enter into bilateral executive agreements with foreign states to facilitate law enforcement data sharing

---

the Academy of European Law Conference on "Prospects for Transatlantic Cooperation on the Transfer of Electronic Evidence to Promote Public Safety" (Apr. 5, 2019), https://www.justice.gov/ opa/ speech/ deputy-assistant-attorney-general-richard-w-downing-delivers-remarks-academy-european-law [hereinafter Downing, ELC speech].

35. CLOUD Act § 103(a)(1), 18 U.S.C. § 2713 (2018). *See generally* Stored Communications Act, 18 U.S.C. §§ 2701–13 (as amended following the CLOUD Act).

36. Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1212 (2004).

37. *Id.* at 1212–13; *see* 18 U.S.C. §§ 2701–03; *e.g.*, United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2011); *In re* Search of Info. Associated with Four Redacted Gmail Accts., 371 F. Supp. 3d 843, 844–46 (D. Or. 2018) (upholding a challenge to an SCA warrant on the basis that it was overbroad).

38. CLOUD Act § 103(a)(1), 18 U.S.C. § 2713.

39. *See generally In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 829 F.3d 197 (2d Cir. 2016); United States v. Microsoft Corp., 138 S. Ct. 356 (2017), *vacated as moot*, 138 S. Ct. 1186 (2018).

40. U.S. WHITE PAPER, *supra* note 9, at 7.

41. *Compare, e.g.*, Roxana Vatanparast, *Data Governance and the Elasticity of Sovereignty*, 46 BROOK. J. INT'L L. 1, 27 (2020) ("The CLOUD Act expanded the territorial reach of the SCA"), *with* Peter Swire & Jennifer Daskal, *Frequently Asked Questions About the U.S. CLOUD Act*, CROSS-BORDER DATA F. (Apr. 16, 2019), https://perma.cc/ V2KY-NAMK (["T]the U.S. CLOUD Act did not expand the territorial reach of U.S. law, under the DOJ's unchanging view and, in the view of the authors, the most likely prior reading of the law.").

42. This extraterritorial scope is broad both relatively, compared with the position previously prevailing following the Second Circuit judgment below, *see* In re *Warrant*, 829 F.3d at 222 ("[T]he SCA does not authorize a U.S. court to issue and enforce an SCA warrant against a United States-based service provider for the contents of a customer's electronic communications stored on servers located outside the United States."), and practically, given the extent to which data relevant to criminal investigations is currently predominantly held by U.S. service providers. *See* Andrew Keane Woods, *Mutual Legal Assistance in the Digital Age*, *in* THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW 661–62 (David Gray & Stephen E. Henderson eds., 2017).

through a new statutory mechanism codified at 18 U.S.C. § 2523.[43] CLOUD Act agreements arise in part from dissatisfaction by law enforcement about the effectiveness of the main existing method that law enforcement have to obtain overseas data: MLA.[44] Like CLOUD Act agreements,[45] MLA "is based on reciprocity"; each state provides the same level of assistance they expect to receive in return.[46] However, access to data through MLA often takes months or even years,[47] in part because an MLA request from one country must normally be reviewed by, and executed under the law of, the state in which the data and/or service provider is based.[48] In contrast, direct access mechanisms claim to "reduce this time period considerably"[49] by allowing their members to use their own local law to compel data from foreign service providers operating in other member states.[50] This article uses the term "foreign service providers" relatively, to refer to providers who are predominantly operating beyond the jurisdiction of a requesting state (which may have some or no connection with that requesting state). This new CLOUD Act mechanism was summarized by Professors Jennifer Daskal and Peter Swire—commonly viewed as "prominent advocates" of this new model[51]—as follows:

> Countries that sign executive agreements with the U.S. no longer need to go through the [MLA] process to request communications content from U.S.-based providers; rather they can, pursuant to a long list of substantive and procedural safeguards, directly request the data from U.S.-based providers, so long as they are seeking the data of foreigners located outside

43. CLOUD Act § 105(a), 18 U.S.C. § 2523.

44. *See generally* NEIL BOISTER, INTRODUCTION TO TRANSNATIONAL CRIMINAL LAW 311–22 (2d ed. 2018) (outlining mutual legal assistance (MLA) and similar mechanisms); U.S. Dep't of Just., Just. Manual § 9-13.000 (2020).

45. CLOUD Act § 105(b), 18 U.S.C. § 2523(b)(4)(I).

46. BOISTER, *supra* note 44, at 311.

47. UK EXPLANATORY MEMORANDUM, *supra* note 27, ¶ 2; U.S. WHITE PAPER, *supra* note 9, at 3; *e.g.*, RICHARD A. CLARKE ET AL., LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES 226–27 (2013) (expressing various concerns with MLA).

48. *See* BOISTER, *supra* note 44, at 311 (noting that a "requested state" during MLA "uses its own power to do something for the requesting state" under its "local law" and that MLA "can be long-winded and bureaucratic").

49. Data Access Agreement Press Release, *supra* note 3.

50. *See, e.g.*, U.S. WHITE PAPER, *supra* note 9, at 11 ("[T]he framework envisaged by the CLOUD Act [is] that each nation would use its own law to access data."); *see also* Richard W. Downing, Deputy Assistant Att'y Gen., Delivering Remarks at the 5th German-American Data Protection Day on "What the U.S. Cloud Act Does and Does Not Do" (May 16, 2019), https://www.justice.gov/opa/speech/deputy-assistant-attorney-general-richard-w-downing-delivers-remarks-5th-german-american [hereinafter Downing, Germany speech].

51. *E.g.*, Haleform H. Abraha, *Law Enforcement Access to Electronic Evidence Across Borders: Mapping Policy Approaches and Emerging Reform Initiatives*, 29 INT'L J.L. INFO. TECH. 118, 136 (2021).

> the United States. Conversely, those governments must commit to ensuring that U.S. law enforcement can directly request communications content from their local providers—also enabling the United States to bypass the otherwise applicable [MLA] process.[52]

B. The U.S.-UK Agreement

The United States and United Kingdom signed the U.S.-UK Agreement in October 2019.[53] Announcing it, (then) U.S. Attorney General William Barr stated that "[t]his agreement will enhance the ability of the United States and the United Kingdom to fight serious crime . . . by allowing more efficient and effective access to data needed for quick-moving investigations."[54] As noted above, the U.S.-UK Agreement is the first and so far only "CLOUD Act" agreement to date, and is yet to come into force.[55] At international law, it will allow each state to directly enforce its own legal orders for preservation, disclosure, and interception of electronic communications against service providers in the other jurisdiction.[56] It achieves this through a "core obligation": each state agrees to remove all "blocking statutes" in their domestic law that may otherwise prevent service providers from lawfully responding to requests from law enforcement.[57] The SCA ordinarily functions as such a blocking statute, normally prohibiting U.S. service providers from disclosing electronic communications content, other than to U.S. law enforcement.[58] The UK Investigatory Powers Act

---

52. Jennifer Daskal & Peter Swire, *A Possible US-EU Agreement on Law Enforcement Access to Data?*, JUST SECURITY (May 21, 2018), https://www.justsecurity.org/ 56527/ eu-agreement- law-enforc ement- access-data/ (emphasis added).

53. U.S.-UK AGREEMENT, *supra* note 2, at 17.

54. Data Access Agreement Press Release, *supra* note 3.

55. *See supra* note 2.

56. U.S.-UK AGREEMENT, *supra* note 2, arts. 1(10)–(11), 2(1), 3(1)–(2), 6(1), 10(1)–(2), 10(6). While this may be the effect of the U.S.-UK Agreement at international law, as explained below at Part III, countries signing such agreements may be constrained from issuing such requests as a matter of domestic law. This point is addressed in relation to the United Kingdom below at Part III and in relation to the United States at Part IV.

57. U.S. WHITE PAPER, *supra* note 9, at 4; UK EXPLANATORY MEMORANDUM, *supra* note 27, ¶¶ 7–8; Data Access Agreement Press Release, *supra* note 3; HL Deb (20 Nov. 2018) (794) cols. 139–40 (UK) (statement of Baroness Williams).

58. 18 U.S.C. §§ 2701–02; *see* STEPHEN P. MULLIGAN, CONG. RSCH. SERV., R45173, CROSS-BORDER DATA SHARING UNDER THE CLOUD ACT 11 (2018) (referring to the overarching legislation containing the SCA and the Wiretap Act, the Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2501 *et seq.* (2018), as a blocking statute). The term "blocking statute" refers to any "conflicting legal obligations" that "prevent disclosure" in this context. *See* U.S. WHITE PAPER, *supra* note 9, at 3, 10–11; UK EXPLANATORY MEMORANDUM, *supra* note 27, ¶ 8. Arguably, given the immunity provisions explored in Part III, the purported effect of the U.S.-UK Agreement is even greater than lifting blocking laws; it also appears to remove the need for service providers to consider any domestic law that would normally govern their conduct when responding to a foreign law enforcement request under a CLOUD Act agreement, including compliance and similar laws that may slow, but not necessarily restrict,

2016 (IPA) operates similarly.[59] As a result, foreign law enforcement seeking data held by service providers subject to U.S. or UK law, respectively, typically need to use MLA.[60]

The U.S.-UK Agreement was subject to negative resolution periods in the UK Parliament and U.S. Congress, although these periods have both expired without objection.[61] Since July 8, 2020, the countries have therefore been free to implement the agreement through an exchange of diplomatic notes.[62] Although the responsible UK Minister announced in September 2020 that implementation was expected by the end of that year,[63] this has been delayed due to data protection concerns, as explained below.[64] At the time of writing, the U.S.-UK Agreement is expected to come into force before the end of 2021.[65]

C. Perceived Impact On U.S. Investigatory Powers

Discussion to date has focused on *incoming* requests to U.S. global service providers from the UK and other foreign states.[66] There has been almost no consideration of how these agreements facilitate *outgoing* U.S.

---

disclosure.

59. Investigatory Powers Act 2016, c. 25, §§ 3, 11 (UK); *see* HL Deb (20 Nov. 2018) (794) cols. 139–40 (UK) (statement of Baroness Williams) (referring to the Investigatory Powers Act as a blocking statute). Other UK laws may have a similar effect. *E.g.*, Computer Misuse Act 1990, c. 18 (UK); *see* LAW COMMISSION, SEARCH WARRANTS, 2020-1, HC 852, ¶ 18.40 (UK); *see also infra* text accompanying notes 133–143.

60. UK EXPLANATORY MEMORANDUM, *supra* note 27, ¶ 2; U.S. WHITE PAPER, *supra* note 9, at 3, 10–11.

61. *See* Paul Greaves & Peter Swire, *New Developments for the UK and Australian Executive Agreements with the U.S. Under the CLOUD Act*, CROSS-BORDER DATA F. (July 19, 2020), https:// www.crossborderdataforum.org/new-developments-for-the-u-k-and-australian-executive-agreements-with-the-u-s-under-the-cloud-act-2/ ("The 180 days for Congress to disapprove the agreement expired on July 8 . . . ."); *Agreement, Done at Washington on 3rd October 2019, Between the Government of the United Kingdom of Great Britain and Northern Ireland and the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime*, UK PARLIAMENT (Jan. 20, 2021), https://api. parliament.uk/view/treaty/bjKV1oDq ("Parliamentary procedure concluded, Government can ratify treaty.").

62. U.S.-UK AGREEMENT, *supra* note 2, art. 16; Greaves & Swire, *supra* note 61.

63. *See* 10 Sept. 2020, Draft Investigatory Powers (Communications Data) (Relevant Public Authorities and Designated Senior Officers) Regulations 2020 Deb (2020) col. 4 (UK) (statement of Minister for Security, James Brokenshire) ("[W]e are now in the final phases of entering the agreement into force, which we expect to happen later this year").

64. *See infra* note 144.

65. *See supra* note 2.

66. *E.g.*, Eddie B. Kim, *U.S.-UK Executive Agreement: Case Study of Incidental Collection of Data Under the CLOUD Act*, 15 WASH. J. L., TECH. & ARTS 247 (2020); PETER SWIRE & JUSTIN HEMMINGS, AM. CONST. SOC'Y, OVERCOMING CONSTITUTIONAL OBJECTIONS TO THE CLOUD ACT 6–14 (2020); Jennifer Stisa Granick & Neema Singh Guliani, *New Bill That Would Give Foreign Governments a Fast Track to Access Data*, JUST SECURITY (Mar. 13, 2018), https:// www.justsecurity. org/ 53705/ bill-give-foreign- governments-fast-track-access-data/.

law enforcement requests to UK service providers.[67] This dearth of commentary appears to have been driven by United States' statements, including in the *White Paper*.[68] Government "white papers" typically outline actual or proposed government policy.[69] Here, the *White Paper*, published by DOJ in April 2019, "describes the interests and concerns that prompted the enactment of the CLOUD Act and provides a concise point-by-point distillation of the effect, scope, and implications of the Act, as well as answers to frequently asked questions."[70] The United States and United Kingdom acknowledge that the U.S.-UK Agreement theoretically provides the United States "reciprocal access, under a U.S. court order, to data from UK[] service providers."[71] However, in the *White Paper* and other statements, these countries suggest that the United States is unlikely to make any significant use of the U.S.-UK Agreement itself, i.e. by using it to request data from UK service providers.[72] The main United States benefit, they say, is that the U.S.-UK Agreement will reduce strain on U.S. MLA processes, as the UK will no longer clog this up with MLA requests for evidence held by U.S. service providers.[73] Professor Theodore Christakis reported that, at an

67. The main exception comprises a series of short blog posts between Albert Gidari and Professor Jennifer Daskal debating the potential for U.S. law enforcement to issue extraterritorial wiretap requests to UK service providers. *See* Albert Gidari, *Can the US-UK CLOUD Act Agreement Be Fixed?*, CTR. FOR INTERNET & SOC'Y (Nov. 18, 2019, 1:07 PM), http://cyberlaw. stanford. edu/ blog/2019/11/can-us-uk-cloud- act-agreement-be-fixed (linking to the earlier blog posts); *see also* Peters et al., *supra* note 7, at, 1092, 1096–98, 1113–15 (providing a high-level analysis of how U.S. prosecutors could hypothetically use the U.S.-UK Agreement to obtain overseas data). There is nonetheless a generalized fear of the United States' potential use of CLOUD Act agreements by many outside the United States, as I have discussed elsewhere. Cochrane, *supra* note 33, at 29–37.

68. *See infra* notes 76–77.

69. *White Paper*, WEBSTER'S NEW INTERNATIONAL DICTIONARY (1993); *e.g.*, Image Online Design, Inc. v. Core Ass'n, 120 F. Supp. 2d 870, 873 n.7 (C.D. Cal. 2000) ("The DOC White Paper is a statement of policy from the United States Department of Commerce"). Perhaps more commonly, a white paper represents an "intermediate" step towards policy development, often publicly released for consultation prior to drafting, rather than, as here, an explanation of a finalized document. *See Paper: White Paper,* BLACK'S LAW DICTIONARY (11th ed. 2019).

70. Press Release, U.S. Dept. of Just., Off. of Public Affs., Justice Department Announces Publication of White Paper on the CLOUD Act (Apr. 10, 2019), https://www.justice. gov/opa/pr/justice-department- announces-publication-white-paper-cloud-act [hereinafter DOJ Announcement].

71. Data Access Agreement Press Release, *supra* note 3; *see also* OFF. OF THE INSPECTOR GEN., DEP'T OF JUST., AUDIT OF THE CRIMINAL DIVISION'S PROCESS FOR INCOMING MUTUAL LEGAL ASSISTANCE REQUESTS AUDIT DIVISION, NO. 21-097, 18 (2021) [hereinafter DOJ IG AUDIT] ("The CLOUD Act requires [its] Agreements to be reciprocal, so the U.S. would also be able to issue requests for data held by CSPs in foreign countries under the Agreements.").

72. UK EXPLANATORY MEMORANDUM, *supra* note 27, at 5; U.S. WHITE PAPER*, supra* note 9, at 5; *see* The Overseas Production Orders and Requests for Interception (Designation of Agreement) Regulations 2020, SI 2020/38, reg. 2(b) (UK) [hereinafter UK Designation Regulations] ("[I]t is anticipated that the [U.S.] will make considerably less use of the Agreement as fewer UK CSPs offer their consumer services on a global basis.").

73. UK EXPLANATORY MEMORANDUM, *supra* note 27, at 5; U.S. WHITE PAPER*, supra* note 9, at 5.

October 2019 public conference, "representatives of [DOJ] could not provide any example where the US, under current law, would need to use the Agreement (instead of the CLOUD Act) to gain access."[74] One of the same DOJ representatives appeared to rationalize this by stating that "the vast majority of major service providers are already in the territory and jurisdiction of the United States."[75]

The United States has expressly denied that its jurisdiction over service providers has been impacted either by the CLOUD Act (typically referring to the SCA's new 18 U.S.C. § 2713)[76] or by agreements made under it.[77] Although the term "jurisdiction" is used in many different ways,[78] jurisdiction in this context refers to whether a U.S. court has "personal jurisdiction" over that provider and thus can legitimately compel compliance by that provider with an SCA order.[79] The United States says that "the CLOUD Act does not expand [U.S.] jurisdiction . . . nor do CLOUD Act agreements create new obligations under U.S. law for service providers," whether U.S. or UK-based.[80] According to the *White Paper*, whether a foreign company is subject to U.S. jurisdiction continues to be a "fact-

74. Theodore Christakis, *21 Thoughts and Questions about the UK-US CLOUD Act Agreement: (and an Explanation of how it Works–with Charts)*, EUR. L. BLOG, (Oct. 17, 2019), https:// europeanlawblog. eu/ 2019/10/17/21-thoughts-and-questions-about-the-uk-us-cloud-act-agreement-and-an-explanation-of-how-it-works-with-charts/ (referencing Richard W. Downing, Deputy Assistant Att'y Gen., Remarks during Privacy + Security Academy Forum Panel: 'Globalization of Criminal Evidence' (Oct. 15, 2019)). The reference to "the CLOUD Act" is presumably to the SCA's new 18 U.S.C. § 2713. *See supra* text accompanying notes 35–38.

75. Downing, ELC speech, *supra* note 34; *see* Woods, *supra* note 42, at 661–62, 663 n.9.

76. U.S. WHITE PAPER, *supra* note 9, at 8, 14, 17 ("[T]he CLOUD Act did not give U.S. courts expanded jurisdiction over companies."); Downing, Germany speech, *supra* note 50 ("Nothing in the Act expands the categories of providers subject to U.S. jurisdiction. Nothing in the Act alters who falls under the jurisdiction of U.S. courts . . . ."). Whether 18 U.S.C. § 2713 had a jurisdictional impact in the (differing) sense of expanding the *scope* of data that SCA orders may compel from providers already subject to U.S. jurisdiction is debated, as noted above. *See supra* note 41.

77. U.S. WHITE PAPER, *supra* note 9, at 5, 13 (stating that "CLOUD Act agreements do not impose any new obligation on *foreign* [service providers] to comply with a U.S. government order" nor "allow the U.S. government to acquire data that it could not before," and they "do not alter the fundamental constitutional and statutory requirements U.S. law enforcement must meet to obtain legal process for that data"); *see also* DOJ Announcement, *supra* note 70 (similar); Downing, Germany speech, *supra* note 50 ("CLOUD Act agreements . . . would not impose any new affirmative obligation either on other countries' providers to comply with U.S. orders, or on U.S. providers to comply with other countries' orders. They simply remove, on both ends, the conflicts of law."); *see* Raman, *supra* note 3 (noting, when comparing CLOUD Act agreements to the proposed EU model, that "[t]he CLOUD Act, by contrast, does not expand jurisdiction over any additional providers.").

78. *See infra* notes 165–167 (outlining differing meanings of jurisdiction in U.S., UK and international law).

79. U.S. WHITE PAPER, *supra* note 9, at 5. I detail U.S. law of personal jurisdiction, as well as the related "subject matter jurisdiction" law, at *infra* Parts III.B(2) and IV.A.

80. U.S. WHITE PAPER, *supra* note 9, at 5, 14.

specific inquiry" that is "based on constraints in the [U.S.] Constitution" requiring "personal jurisdiction" that remain unaltered by the CLOUD Act or the U.S.-UK Agreement.[81] Elaborating on these in the context of the CLOUD Act, the United States has commented:

> The principles of personal jurisdiction are rooted in the U.S. Constitution and a well-developed body of constitutional law, and they provide for a strict test before a U.S. court can determine that a particular entity has 'sufficient minimum contacts' with the United States based on the nature, quantity, and quality of those contacts. Those principles are unchanged.[82]

The United States' position is that "[t]he only legal effect of a CLOUD [Act] agreement is to eliminate the legal conflict for qualifying orders."[83] Its claims about the jurisdictional impact of both the CLOUD Act and potential CLOUD Act agreements have been repeated in various commentaries and appear to be widely accepted.[84]

---

81. *Id.* at 8.

82. Downing, Germany speech, *supra* note 50.

83. U.S. WHITE PAPER, *supra* note 9, at 5.

84. *E.g.*, Caitlin Potratz Metcalf and Peter Church, *U.S. CLOUD Act and GDPR – Is the Cloud Still Safe?*, LINKLATERS: DIGILINKS (Sept. 13, 2019), https://www.linklaters.com/ en/insights/blogs/ digilinks/ 2019/ september/us-cloud-act-and-gdpr-is-the-cloud-still-safe ("[T]he [CLOUD] Act does not impose new obligations on U.S. or foreign communication service providers"); NATASCHA GERLACH & ELISABETH MACHER, CLEARY GOTTLIEB, EUROPEAN DATA PROTECTION AUTHORITIES EXPLORE U.S. CLOUD ACT'S POTENTIAL IMPACT ON THE GDPR 2 (2019), https://www.clearygottlieb.com/-/media/ files/ alert-memos-2019/us-cloud-acts-potential-impact-on-the-gdpr.pdf ("According to the DOJ, even with the CLOUD Act, much remains the same, including . . . the fact-specific analysis a U.S. court must undertake to determine whether it has personal jurisdiction . . . ."); *id.* ("[T]he DOJ has also emphasized that an executive agreement in and of itself would not . . . establish the U.S. Government's . . . jurisdiction over service providers . . . ."); Alexis Collins & Destiny D. Dike, *DOJ Releases White Paper Addressing Scope & Implications of CLOUD Act*, CLEARY CYBERSEC. & PRIV. WATCH (Apr. 18, 2019), https://www.clearycyberwatch.com/2019/04/doj-releases-white-paper-addressing-scope-implications-of- cloud-act/ ("The DOJ's white paper argues that the CLOUD Act clarifies [service providers]' disclosure obligations without expanding the U.S. government's jurisdiction over foreign companies."); Bruce Zagaris, *U.S. Department of Justice Publishes White Paper on the Cloud Act*, 35 INT'L ENFORCEMENT L. REP. 150, 151 (2019) ("The only legal effect of a CLOUD agreement is to eliminate the legal effect for qualifying orders."); Jim Garland, Trisha Anderson & Alexander Berengaut, *Department of Justice Releases White Paper on CLOUD Act*, COVINGTON: INSIDE PRIV. (Apr. 11, 2019), https://www.insideprivacy.com/cloud-computing/department-of-justice-releases-white-paper-on-cloud-act/ #more-9841 ("[T]he FAQ responses note that the CLOUD Act did not give U.S. courts expanded jurisdiction over companies."); Alexander A. Berengout & Lars Lensdorf, *The CLOUD Act at Home and Abroad*, 20 COMPUT. L. REV. INT'L 111, 113 (2019) ("[T]he [*White Paper*] state[s] that the CLOUD Act did not give U.S. courts expanded jurisdiction over non-U.S. persons."); Paul M. Schwartz, *Legal Access to the Global Cloud*, 118 COLUM. L. REV. 1681, 1751 n.462 (2018) (noting that, under the CLOUD Act regime, the U.S. may compel service providers in foreign CLOUD Act regime member states to conduct wiretaps but "[t]hese foreign service providers must, however, be otherwise subject to the jurisdiction of U.S. wiretap orders."); *see* Swire & Daskal, *supra* note 41 (implying at Q10 and Q15 that direct U.S. requests to a foreign service provider require that provider to already have "sufficient business or other contacts with the U.S. to establish jurisdiction"). *But see also infra* note 89.

Although the CLOUD Act, U.S.-UK Agreement, and the *White Paper* were all produced under the Trump Administration—and policies and priorities frequently change between administrations[85]—President Joe Biden reiterated his commitment to the U.S.-UK Agreement in June 2021 in a joint public statement with UK Prime Minister Boris Johnson.[86] The *White Paper* and related materials remain "official CLOUD Act-related materials" on DOJ's website.[87] There is therefore every indication that the new Administration similarly considers that CLOUD Act agreements do no more than lift conflicts.[88] A relatively more nuanced position has been set out by Jennifer Daskal—one of the main academics to have analyzed the CLOUD Act. Daskal acknowledges that, under CLOUD Act agreements, "the United States could, in theory, compel production of certain communications content from providers based in partner foreign countries."[89] Daskal says, however, that "explicit legal authority in U.S. law" would be necessary to "enable issuance of these kind of extraterritorial disclosure orders" and that as of now, no such explicit authority exists.[90] This article returns to these

85. *E.g.*, Memorandum from Acting Attorney General to All Federal Prosecutors (Jan. 29, 2021), https:// www.justice.gov/ag/page/file/1362411/download (announcing the rescission and replacement of the DOJ charging and sentencing policy).

86. *See Joint Statement on the Visit to the United Kingdom of the Honorable Joseph R. Biden Jr. President of the United States of America at the Invitation of the Rt. Hon. Boris Johnson M.P. the Prime Minister of the United Kingdom of Great Britain and Northern Ireland*, WHITE HOUSE (June 10, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/10/joint-statement-on-the-visit-to-the-united-kingdom-of-the-honorable-joseph-r-biden-jr-president-of-the-united-states-of-america-at-the-invitation-of-the-rt-hon-boris-johnson-m-p-the-prime-min/ (stating that "we look forward to bringing into force a robust bilateral data access agreement" referring to the U.S.-UK Agreement).

87. *CLOUD Act Resources*, U.S. DEP'T OF JUST. (Aug. 20, 2021), https://www. justice. gov/ dag/ cloudact (listing the *White Paper* and, separately, the frequently asked questions also included as part of the *White Paper*, as official documents).

88. *See* U.S. WHITE PAPER, *supra* note 9.

89. Jennifer Daskal, *Privacy and Security Across Borders*, 128 YALE L.J. F. 1029, 1041 (2019); *see also, e.g.*, Ben Barnett, Caroline Black & Laura Manson, *Overseas Production Orders – Where Are We Now?*, DECHERT LLP (Nov. 23, 2020), https://www.dechert.com/knowledge/ onpoint/2020/11/overseas-production-orders—-where-are-we-now-.html ("As yet, the U.S. has not passed domestic legislation which would create reciprocal rights for U.S. authorities to obtain data from UK CSPs under the Agreement."); *see* Alison Geary & Joanna Howard, *Apples and Oranges: UK-US Bilateral Data Access Agreement Comes into Effect*, WILMERHALE (Aug. 11, 2020), https://www.wilmerhale.com/ en/ insights/blogs/wilmerhale-w-i-r-e-uk/20200811-apples-and-oranges-uk-us-bilateral-data-access-agreement-comes-into-effect (stating that, "despite [the] reciprocity" of the U.S.-UK Agreement, "[f]or the US, there is no new process for seeking data overseas enacted into legislation").

90. Daskal, *Privacy and Security*, *supra* note 89 at 1041 ("The CLOUD Act does not provide any."); *see also* Jennifer Daskal, *Setting the Record Straight: the CLOUD Act and the Reach of Wiretapping Authority Under US Law*, CROSS-BORDER DATA F. (Oct. 1, 2018), https:// www. cross borderdataforum.org/setting-the-record-straight-the-cloud-act-and-the-reach-of-wiretapping-authority-under-us-law/ ("The executive agreements envisioned by the CLOUD Act do not provide any independent authority to conduct wiretaps or other surveillance."); Jennifer Daskal, *Correcting the Record: Wiretaps, the CLOUD Act, and the US-UK Agreement*, JUST SECURITY (Oct. 31, 2019), https://

points—evaluating, at U.S. law, the relevance of the *White Paper* and/or whether additional legislative authority would be necessary to issue extraterritorial requests—below.[91] Before considering the impact of CLOUD Act agreements at U.S. law, however, it is appropriate to first look at the international plane.

III. JURISDICTIONAL BENEFITS OF CLOUD ACT AGREEMENTS AT INTERNATIONAL LAW

Part III explains that direct access agreements like the U.S.-UK Agreement provide their member states with at least two international law benefits. International law can be subdivided into "private" and "public" realms.[92] Private international law, also known as "conflict of laws," "resolv[es] controversies between private persons . . . primarily in domestic litigation, arising out of situations having a relationship to more than one state."[93] Public international law, also known simply as "international law," regulates "the conduct of states and international organizations."[94] The U.S.-UK Agreement appears to give jurisdictional benefits to its members in each realm. Addressing these, Part III argues that U.S. law enforcement have good reasons to take advantage of each benefit, focusing on stored data requests under the SCA.[95]

---

www.justsecurity.org/66774/correcting-the-record-wiretaps-the-cloud-act-and-the-us-uk-agreement/ (arguing that, "while . . . the [U.S.-UK] Agreement provides for reciprocal access in theory, there is no reciprocal change in practice" because "[t]here are no affirmative authorities . . . to enable the [U.S.] to compel assistance by foreign-based providers that are not otherwise subject to U.S. jurisdiction").

91. *See infra* Parts IV.C and IV.D.

92. RESTATEMENT (THIRD) OF FOREIGN RELS. L. OF THE U.S. § 101 (AM. LAW. INST. 1987); JAMES CRAWFORD, BROWNLIE'S PRINCIPLES OF PUBLIC INTERNATIONAL LAW 458 (9th ed. 2019).

93. RESTATEMENT (THIRD) OF FOREIGN RELS. L. OF THE U.S. § 101; *see also* CRAWFORD, *supra* note 92, at 458.

94. RESTATEMENT (THIRD) OF FOREIGN RELS. L. OF THE U.S. § 101; *see* CRAWFORD, *supra* note 92, at 3–11 (discussing the history of [t]he law of nations, now known as (public) international law").

95. Stored Communications Act, 18 U.S.C. §§ 2703, 2713. This Part II assumes that the United States can use the SCA to request data from foreign service providers, *see supra* note 7. *But see also infra* Part IV.B. Although outside the scope of this article, the U.S.-UK Agreement also empowers the United States (and UK) to directly enforce intercept or "wiretap" requests against foreign service providers. *See* U.S.-UK AGREEMENT, *supra* note 2, art. 1(10)–(11) (defining "Legal Process" and "Order" to include preservation and intercept requests). *See generally* Wiretap Act, 18 U.S.C. §§ 2510–23 (comprising the U.S. intercept statute). The Pen Register and Trap and Trace Act, 18 U.S.C. §§ 3121–27, is also within the scope of CLOUD Act executive agreements. *See* CLOUD Act § 104 (incorporated at 18 U.S.C. §§ 3121(a), 3124(d)–(e)) (amending that legislation to effect this).

A. Private International Law: Minimizing Conflicts

(1) How CLOUD Act Agreements Minimize Conflicts Of Laws

The primary claimed benefit of CLOUD Act agreements—minimizing conflicts of law—is readily acknowledged by the United States. As it explains:

> [W]e live in a world of conflicting cross-currents – the simultaneous need to reach out for data stored abroad and concern about limiting the ability of others to reach in. And these contradictory pressures create a global landscape rife with potential conflicts of law. The global technology companies that hold electronic evidence are frequently subject to more than one country's laws. All too often, one country may order them to disclose data needed for an investigation, while another country's laws may "block" disclosure of that same data. It is a constant push and pull.[96]

"The U.S. Congress enacted the CLOUD Act as a way [to] reduce [these] conflicts of law," the United States has remarked[97]—although the broad extraterritorial scope of the CLOUD Act's first accomplishment, new 18 U.S.C. § 2713, risks precisely the opposite, i.e. intensifying conflicts.[98] While this is concerning,[99] this article focuses on the CLOUD Act's second accomplishment, bilateral CLOUD Act agreements. In contrast to § 2713 of the SCA, CLOUD Act agreements have the potential to reduce conflicts. In particular, through these agreements, "[b]oth countries can agree to eliminate the conflicts of law so that both countries can more efficiently obtain the information needed to protect their citizens."[100] For example, the SCA, which creates criminal offenses and civil remedies for wrongful disclosure of communications processed by service providers,[101] currently "stand[s] in

96. Downing, Germany speech, *supra* note 50; *see* DAVID ANDERSON, A QUESTION OF TRUST: REPORT OF THE INVESTIGATORY POWERS REVIEW 204 (2015) ("[S]ervice providers operating internationally . . . do not see it as their role to resolve the conflicts of jurisdiction that arise . . . But the reality is that providers are at the centre of resolving those conflicts on a daily basis.").

97. Downing, Germany speech, *supra* note 50; *see also id.* (referring to CLOUD Act agreements "as a Respite from Conflicts"); Daskal, *Privacy and Security*, *supra* note 89, at 1036 n.25 ("[T]he whole point of becoming a qualifying foreign government [under the CLOUD Act regime] is to minimize legal conflict").

98. I argue elsewhere that the new 18 U.S.C. § 2713 is an example of a "unilateral assertion of extraterritorial jurisdiction" that risks exacerbating conflicts between jurisdictions. Cochrane, *supra* note 33, at 20 (quoting Jennifer Daskal, *Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues*, 8 J. NAT'L SECURITY L. & POL'Y 473, 477–78 (2016)). Tellingly, this prospect was emphasised before the Supreme Court in *Microsoft Ireland* prior to the passage of the CLOUD Act. *See, e.g.*, Brief for the New Zealand Privacy Commissioner as *Amicus Curiae* in Support of Neither Party at 13–14 , U.S. v Microsoft, 138 S. Ct. 1186 (2018) (No 17-2) (noting, prior to the enactment of the CLOUD Act that, applying the SCA "to date held in Ireland" or "in New Zealand" could "create a conflict" and "risk a lack of clarity and so risk uncertainty and [further] conflict").

99. *Id.*

100. Downing, Germany speech, *supra* note 50.

101. Stored Communications Act, 18 U.S.C. § 2701(a) (creating a criminal offense prohibiting

the way of [U.S.] providers complying with lawful orders from" the United Kingdom for the contents of communications.[102] While the SCA permits, and in certain scenarios compels, service providers regulated by U.S. law to disclose communications to law enforcement and other governmental entities, these exemptions do not apply to foreign governments.[103] The SCA instead acts as a blocking statute for U.S. service providers and foreign governments, enacting a "presumptive ban on the disclosure of contents of communications" from such providers overseas.[104]

The SCA's blocking provisions will now fall away when UK law enforcement request data through the U.S.-UK Agreement.[105] UK law enforcement may freely issue requests under their own law for such data to U.S. service providers, and U.S. service providers need not worry that responding may breach the SCA. The intention is that "[t]he only law governing the disclosure would be the law of the country issuing the order."[106] As a result, other than (under current law) merely theoretical Fourth Amendment liability,[107] providers will apparently be immunized altogether under U.S. law for responding to such requests.[108] Pursuant to new

certain "intentional[] access[]" to electronic communications held by providers subject to the SCA); *id.* § 2707 (allowing aggrieved persons to recover "such relief as may be appropriate," including damages, "in a civil action" from providers and others for "knowing or intentional" SCA violations); *see* Van Alstyne v. Elec. Scriptorium, Ltd., 560 F.3d 199, 204–05 (4th Cir. 2009) (outlining the damages that aggrieved persons may recover under 18 U.S.C. § 2707(c)); *e.g.*, Cardinal Health 414, Inc. v. Adams, 582 F. Supp. 2d 967, 977 (M.D. Tenn. 2008) ("[Defendant] plainly violated the SCA as a matter of law.").

102. *See* Downing, Germany speech, *supra* note 50.

103. This article focuses on requests for content data, for which the SCA generally acts as a blocking statute for foreign law enforcement. In contrast, where non-content data is requested, service providers may conversely have greater freedom to disclose directly to foreign law enforcement than they do to U.S. law enforcement. *See* Stored Communications Act, 18 U.S.C. 2702(a)(3), (c)(6), 2711(4); MULLIGAN, *supra* note 58, at 4–5; *see also* Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 PENN. L. REV. 373, 409 (2014).

104. *See* Kerr, *supra* note 103, at 409–10.

105. CLOUD Act, §§ 104(2)(A)(i)(II), 104(2)(B), 18 U.S.C. §§ 2702(b)(9), 2707(e)(3).

106. Downing, Germany speech, *supra* note 50; *see also* Evan Norris & Morgan J. Cohen, *How US Authorities Obtain Foreign Evidence in Cross-Border Investigations*, *in* AMERICAS INVESTIGATIONS REVIEW 2021 25 (2020) ("Because the CLOUD Act removes [U.S.] legal prohibitions on disclosing electronic information in response to [UK]-issued legal process, a [UK] reviewing court would not need to engage in a conflict of laws analysis.").

107. *See* Hepting v. AT&T Corp., 439 F. Supp. 2d 974, 995 (N.D. Cal. 2006) (suggesting it is doubtful that SCA's immunity provisions could exempt persons from Fourth Amendment liability). *But see* Marshall v. Willner, No. CIV A 3:06CV-665-M, 2007 WL 2725971, 5 (W.D. Ky. Sept. 14, 2007) (reaching the opposite conclusion). However, good faith compliance on 18 U.S.C. § 2702(b)(9), *see infra* notes 109–110, has been found to fulfill the Fourth Amendment. Thompson v. Platt, 815 F. App'x 227, 238–39 (10th Cir. 2020). In any event, Constitutional claims require "state action" but "a private party's mere compliance with a court order does not constitute state action." *Id.* at 238. *See also* Patricia L. Bellia, *Chasing Bits Across Borders*, 2001 U. CHI. LEGAL F. 35, 99 ("Under state action principles, foreign conduct authorized by an international agreement will be attributable to the United States.").

108. *See infra* text accompanying notes 115–117. Similar statutory immunities are provided when

18 U.S.C. § 2702(b)(9), providers will be exempt from civil liability when responding to UK law enforcement data requests.[109] A mere "good faith reliance" on 18 U.S.C. § 2702(b)(9) provides "a complete defense to any civil or criminal action brought under this chapter or any other law."[110] On their face, these provisions are expressly designed to protect providers.[111] In addition to CLOUD Act agreements directly reducing conflicts in this way, an area for further study is whether the process of negotiating such agreements may indirectly reduce conflicts and related concerns between states. It is claimed, for example, that the United Kingdom enacted changes to the IPA during U.S.-UK Agreement negotiations to pacify United States objections to this legislation.[112]

U.S. service providers intercept or provide other data to foreign law enforcement pursuant to CLOUD Act agreements. *See* ORIN S. KERR, COMPUTER CRIME LAW 107 (4th ed. Supp. 2020) (noting that "the CLOUD Act adds new exceptions to each of three major federal statutory surveillance laws for conduct in response to foreign legal process" and describing these).

109. 18 U.S.C. § 2703 ("No cause of action shall lie in any court against any provider . . . for provider information, facilities, or assistance in accordance with the terms of a . . . statutory authorization . . . under this chapter."); *see* Wilson v. Nextel Commc'n, 296 F. Supp. 3d 56, 59 (D.D.C. 2017) (holding providers become "not subject to suit" where 18 U.S.C. § 2703 applies); *In re* United States, 157 F. Supp. 2d 286, 289 (S.D.N.Y. 2001) ("The provider . . . is shielded from liability for any claim"); Alexander v. Verizon Wireless Servs., 875 F.3d 243, 250 (5th Cir. 2017) ("[18 U.S.C.] § 2703(e) provides immunity to a service provider when it makes a disclosure in accordance with a provision of the SCA."). New 18 U.S.C. § 2702(b)(9) is a "statutory authorization." *See* 18 U.S.C. § 2702(b)(8) (a similarly worded statutory authorization); *In re* United States, 352 F. Supp. 2d 45, 46–47 (D. Mass. 2005) (holding 18 U.S.C. § 2702(b)(8) was also a statutory authorization caught by 18 U.S.C. § 2703).

110. 18 U.S.C. § 2703(e)(3); *see* Conley v. Turquand, No. A-07-CA-188-SS, 2008 WL 11404534, at *2 (W.D. Tex. Mar. 11, 2008) (recording counsel submission of this section as a "safe harbor"); Hepting v. AT & T Corp., 439 F. Supp. 2d 974, 1002 (N.D. Cal. 2006) (citing S. REP. NO. 99–541, at 26, *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3580) (commenting that this requires only "a facially valid court order"); *e.g.*, Villa v. Maricopa City, 865 F.3d 1224, 1236–37 (9th Cir. 2017) (under equivalent Wiretap Act laws, holding that "rights . . . were violated in two respects, but both violations were in good faith within the meaning of" statutory provisions).

111. They may therefore incentivize providers not to investigate orders beyond determining these are facially valid. *See* United States v. Rodriguez, No. 17-cr-10066-IT, 2018 WL 988054, at *4 (D. Mass. Feb. 20, 2018) ("It is for the court, and not the service provider, to decide whether interception is warranted."); Sukkar v. USA Mobility, Inc., NO. MJG-06-848, 2006 WL 8456781, at *3 (D. Md. Sept. 20, 2006) ("Nor does the [SCA] require the provider of the information to engage in litigation regarding the validity of an order with which it complies.").

112. Raman, *supra* note 3 ("[T]he United Kingdom undertook changes to its own laws in order to assure that it could comply with the CLOUD Act's requirements."). Linked to this, the CLOUD Act requires that the U.S. Attorney-General must first provide "a written certification and explanation" to Congress on the sufficiency of the laws of a proposed CLOUD Act agreement signatory state in certain areas, including civil liberties, at least 180 days before the agreement comes into force. CLOUD Act § 105(a), 18 U.S.C. 2523(b)–(d) (2018); *see, e.g.*, CLOUD Act; Attorney General Certification and Determination, 85 Fed. Reg. 12578-01 (Mar. 3, 2020) (notification of the U.S.-U.K. Agreement certification). The impact of what appear to be U.S. 'adequacy' mechanisms both here and in related areas also deserves additional consideration.

In any event, this direct "minimizing conflicts" benefit applies equally to U.S. law enforcement, whether they are seeking data from service providers solely operating in the United Kingdom,[113] or from service providers over which multiple states claim jurisdiction—including the "global technology companies" like Google, Facebook, and Amazon that operate in many jurisdictions.[114] Putting aside potential personal jurisdiction objections—considered separately at Part IV below—when served with an SCA order from U.S. law enforcement, providers may currently theoretically raise a "comity" (i.e. conflicts of law) defense,[115] on the basis that to provide the data would breach a foreign law like the United Kingdom IPA, which creates criminal offenses and civil remedies similar to the SCA.[116] However, UK law blocking provisions will also drop away when U.S. law enforcement requests are made pursuant to the U.S.-UK Agreement.[117] The United Kingdom has "designated" the U.S.-UK Agreement as a "relevant international agreement" under section 52 of the IPA.[118] Through this designation, section 52 provides "the gateway for the flow of information from the UK to the United States."[119] Service providers subject to UK law may then process data for foreign law enforcement,[120] so long as "the interception is carried out in response to a request made in accordance with a relevant international agreement by the competent authorities of a country

113. Whether U.S. law permits data requests to providers regulated solely by UK law, given personal jurisdiction requirements in the Fifth Amendment's Due Process clause, is addressed in Part IV of this article.

114. *See* Downing, Germany Speech *supra* note 50; *see also supra* note 96 and accompanying text.

115. *See* CLOUD Act § 103(c), Pub. L. No. 115–141, 132 Stat. 1213 (2018) (recognizing a common law comity defense to SCA orders). *See generally* Societe Nationale Industrielle Aerospatiele v. U.S. Dist. Ct. for S. Dist. of Iowa, 482 U.S. 522, 544(1987) (setting out the common law test for raising a conflict of laws objection under U.S. law).

116. Investigatory Powers Act 2016, c. 25, § 3 (UK) (concerning criminal offenses); *id.* § 8 (concerning civil remedies); *see* HOME OFF., INTERCEPTION OF COMMUNICATIONS: CODE OF PRACTICE 15–16 (2018) (UK) (summarizing these provisions); *e.g.*, R v. Sargent [2001] UKHL 54, [2003] AC 347 [7], [26] (appeal taken from Eng.) (noting that "in carrying out the intercept," party "had committed an offence" of unlawful interception of a "public telecommunication system" under predecessor legislation).

117. *See supra* note 110.

118. UK Designation Regulations, supra note 72, reg. 2(b).

119. HL Deb (11 Feb. 2019) (795) col. 1671 (UK) (statement of Baroness Williams); UK Designation Regulations, supra note 72, Explanatory Memorandum, ¶¶ 7.2, 7.4 (noting that, just as the U.S.-UK Agreement "remove[s] the barriers in [U.S.] law to [U.S. service providers] acting upon UK orders," it "will also enable [U.S.] law enforcement to make requests directly to UK [service providers] for data").

120. Investigatory Powers Act 2016, c. 25, §§ 4, 52 (UK); *see id.* Explanatory Notes ¶ 41 ("[I]nterception of a communication . . . includes accessing stored communications . . . such as messages stored on phones, tablets, or other devices whether before or after they are sent."); *see also* HL Deb (20 Nov. 2018) (794) cols. 140–41 (statement of Baroness Williams).

or territory outside the United Kingdom."[121] This is again specifically intended to immunize service providers from all UK law liability, whether civil or criminal, when responding to requests under the U.S.-UK Agreement.[122] Through section 6 of the IPA, providers' acts become lawful under the IPA and "for all other purposes" under UK law.[123] The House of Lords (now replaced by the UK Supreme Court) has ruled that the predecessor provision to section 6 must be given full force.[124] As a result, like the equivalent SCA position, providers relying on good faith that a request appears to comply with the U.S.-UK Agreement, and therefore section 52, appear immune from UK law liability,[125] other than currently

121. Section 52 provides other threshold requirements, such as requiring that requests must target a person believed to be outside the United Kingdom, Investigatory Powers Act § 52(4), but these are redundant in this context, as they mirror requirements in the U.S.-UK Agreement itself. *See, e.g.*, U.S.-UK AGREEMENT, *supra* note 2, arts. 1(6), 1(12), 4(3)–(4) (prohibiting the United States from "intentionally target[ing] persons in the United Kingdom). Although subsection (5) permits "further conditions" to be specified in regulations, no such regulations currently exist.

122. HL Deb (19 Oct. 2016) (774) col. 2392 (UK) (statement of Earl Howe) ("[This provision] . . . provid[es] reassurance for telecommunications operators that, when conduct is carried out in accordance with the requirements of a notice, the operator will not risk being found to be in breach of any other legal requirement."); Investigatory Powers Act 2016, Explanatory Notes, ¶ 46 (similar); *see* Graham Smith, *The UK Investigatory Powers Act – What It Means for Your Business*, 17 PRIV. & DATA PROT. 9, 10 (2016) ("A small ISP will benefit from the same broader lawful authority purposes as a large provider."). Providers may therefore again be incentivized not to look behind a facially valid order, *see supra* note 111, as appears to be their preference. ANDERSON, *supra* note 96, ¶ 11.32 ("UK companies were generally united [in saying that they did] not wish to have a discretion to question the merits of a particular interception or data request.").

123. Investigatory Powers Act 2016, c. 25, §§ 6 (1)(b), (2), (3)(b).

124. *In re* McE [2009] UKHL 15, [2009] AC 908 [61]–[62], [65] (holding that predecessor legislation "must be taken to mean what it says"). The House of Lords' reasoning is binding upon, and has been followed by, subsequent UK courts. *E.g.*, R v. Palmer [2014] EWCA (Crim) 1681 [31]–[36] (Eng.); A.J.A. v. Comm'r of Police for the Metropolis [2013] EWCA (Civ) 1342 [31]–[32], [2014] WLR 285 (Eng.).

125. *See* Priv. Int'l v. Sec'y of State for Foreign and Commonwealth Aff. [2016] UKIPTrib 14_85-CH [18](i), [20], *overruled on other grounds by* [2021] EWHC (Admin) 27, [2021] 2 WLR 970 ("No act done pursuant to those sections can be unlawful either civilly or criminally."); Harmes v. R. [2006] EWCA (Crim) 928 [15] (noting an equivalent predecessor section "sanctions the legality of the conduct") (Eng.); SIMON MCKAY, COVERT POLICING ¶¶ 7.105, 7.107 (2d ed. 2015) ("Once a court is satisfied that the [request] was properly [made] and the conduct did not exceed its terms, any attack on its lawfulness ought to be impermissible."); Simon McKay, *Lawful Surveillance*, COVERT POLICING L. BLOG (Jan. 16, 2016), https:// simonmckay.co.uk/lawful-surveillance/ (noting that it "creates a shield"); *see also, e.g.*, R (NTL Group Ltd.) v. Ipswich Crown Court [2002] EWHC (Admin) 1585 [24]–[25], [2003] QB 131 (Eng.) (holding that "no offence will . . . be committed" where a service provider responded to an law enforcement statutory request" that provided "lawful authority").

theoretical liability under the European Convention on Human Rights (ECHR)[126] similar to the equivalent U.S. law position.[127]

(2) "Minimizing Conflicts" Is A Significant Benefit For U.S. Law Enforcement—Although Potential GDPR Conflicts Raise Further Questions

U.S. law enforcement should be assumed to have the motivation to channel SCA requests through the U.S.-UK Agreement to minimize conflicts. Various service providers over which the United States asserts jurisdiction, including global service providers, also operate in the United Kingdom.[128] These providers may reasonably fear that SCA requests will breach UK law, such as the IPA's blocking provisions—these are ambiguous but may well be triggered for these providers by requests when data is stored in, or otherwise connected to, the United Kingdom.[129] The growth of

126. Under ECHR Article 8, protecting privacy and related areas, similar analysis applies as under the Fourth Amendment. Convention for the Protection of Human Rights and Fundamental Freedoms [ECHR], Nov. 4, 1950, 213 U.N.T.S. 221; *see supra* note 107. Sections 6 and 52 cannot directly immunise conduct that otherwise breaches Article 8, *e.g.*, RE v. United Kingdom, 63 Eur. Ct. H.R. 2 ¶ 143 (2016) (finding a breach of Article 8 notwithstanding a predecessor immunity provision), and good faith compliance with the IPA would not necessarily fulfill Article 8's requirements, *e.g.*, *id.* at 121, 142, 143 (holding that, although the conduct "had a basis in domestic law," the measures "did not meet the requirements of Article 8 § 2"). However, Article 8's obligations only directly limit interferences by "public authorities," and service providers are generally considered to fall outside its scope. *E.g.*, Richardson v. Facebook [2015] EWHC (QB) 3154 [51]–[63]. *But see* Allison M. Holmes, *Private Actors or Public Authority? How the Status of Communications Service Providers Affects Human Rights*, 22 COMMC'NS. L. 21 (2017) (suggesting providers should be treated as public authorities for this purpose).

127. *See supra* note 107.

128. *See, e.g.*, Raj Bala et al., *Magic Quadrant for Cloud Infrastructure and Platform Services*, GARTNER (Sept. 1, 2020), https:// www.gartner. com/en/documents/3989743/magic-quadrant-for-cloud-infr astructure-and-platform-ser (noting that major service providers operating in the United States, including Amazon Web Services [AWS], Google, IBM, Microsoft, and Oracle, have data centers in the United Kingdom). *See generally ICO's Priorities and Impact of our Work*, INFO. COMM'R'S OFF. (July 31, 2021), https://ico.org.uk/ about- the-ico/news- and-events/ news-and-blogs/2021/07/ico-s-priorities-and - impact-of-our-work (UK) ("Tech companies based across the world have a huge presence in the UK, processing UK citizens [sic] data.").

129. The IPA is "very complex," R v. A [2021] EWCA (Crim) 128, [2021] 2 WLR 1301 [53], but global service providers may breach its prohibition on unlawful interception by responding directly to SCA requests in certain circumstances. First, the requested data must be communications content (or related data) transmitted via a "public telecommunications system," meaning equipment in or controlled from the United Kingdom, used to provide services to people there. Investigatory Powers Act 2016, c. 25, § 3(1)(a)(i) (UK); *see id.* § 261(8)–(13) (defining public "telecommunications system" and related terms); LAW COMMISSION, *supra* note 59, ¶ 16.84 ("The IPA covers any telecommunications operator which provides services to persons within the UK, thereby establishing a necessary jurisdictional connection."); INTERCEPTION OF COMMUNICATIONS, *supra* note 116, ¶¶ 2.4–2.8 (summarising these). Global service providers provide services to United Kingdom persons using equipment located in the United Kingdom over which communications and related data may be transmitted. *See supra* note 128. Secondly, the SCA request must require a "relevant act" to be "carried out by conduct in the United Kingdom," including "modifying, or interfering with, the system or its operation" or "monitoring transmissions made by means of the system." Investigatory Powers Act 2016 §§ 4(2), (8)(a). The meaning

blocking statutes generally have led to predictions of "greater difficulties for U.S. parties who seek access to data in non-U.S. clouds."[130] To the extent these difficulties are caused by UK laws, the U.S.-UK Agreement provides a tailor-made and simple solution: to avoid such conflicts when serving an SCA order on a service provider, all that is required is an additional "certification" from DOJ stating that the order is being issued under, and complies with, the U.S.-UK Agreement and applicable U.S. law.[131] The ease at which this may occur, and the benefits U.S. law enforcement gain from doing so where there is otherwise a risk of UK law conflicts, suggests they will do so as a matter of course.[132]

What is perhaps the most significant blocking statute, the EU General Data Protection Regulation (GDPR or EU GDPR), bears mention. Although the United Kingdom has left the European Union following Brexit, the GDPR has been incorporated within domestic UK law as the "UK GDPR,"[133] and is an example of "retained EU law."[134] Both the EU and UK GDPR comprise "a broad set of privacy regulations governing the collection and use of data."[135] The EU Court of Justice (CJEU), which definitively

of "relevant act" is unclear, *R v. A* [2021] EWCA (Crim) 128 [32], [52]–[53], but the mere extraction of data from a UK server may contribute to or fulfil this requirement. *See id.* (noting that this was considered relevant by the first instance court but not determining "whether the judge was right"). In any event, some providers require local (or regional) access to data stored on such infrastructure, which may be further "conduct in the United Kingdom." *See* Schwartz, *supra* note 84, at 1697 ("[C]loud services offered by AWS and Microsoft's regional European Union cloud are not accessible from the United States.").

130. Schwartz, *supra* note 84, at 1740–41 (noting predictions of "greater difficulties for U.S. parties who seek access to data in non-U.S. Clouds," due to "conflicting rules" internationally); *see also infra* note 155 (discussing predictions of conflicts with the EU GDPR in particular).

131. U.S.-UK AGREEMENT, *supra* note 2, arts. 1(8), 1(11), 5(5), 5(7); *see* Designated Authority under Executive Agreements on Access to Data by Foreign Governments, 28 C.F.R. § 0.64–6 (2020) (authorizing certain DOJ officials to act as "designated authority" under the U.S.-UK Agreement).

132. *See also infra* notes 224–226 and accompanying text (noting that the United States is currently actively devoting resources to issuing requests under CLOUD Act agreements, further suggesting that it will make regular use of these agreements).

133. Data Protection Act 2018, c. 12 (UK); Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019, SI 2020/1586, regs. 2–3 (incorporating the GDPR at UK law as the "UK GDPR."); *see* Rondón v. LexisNexis Risk Solutions UK Ltd. [2021] EWHC (QB) 1427 [14], *appeal pending*, A2/2021/1093 (Jan. 25 or 26, 2022). *See generally* ROSEMARY JAY, DATA PROTECTION: LAW AND PRACTICE ¶¶ 1–074 to 1–084 (Sweet & Maxwell, 5th ed. 2020) (summarizing these arrangements).

134. European Union (Withdrawal) Act (EUWA) 2018, c. 16, §§ 6, 7 (UK); *see* Lipton v. BA City Flyer Ltd. [2021] EWCA (Civ) 454 [52]–[83], [2021] 1 WLR 2545 (elaborating on the interpretation of EUWA and providing "basic principles" for interpreting EU law within UK courts after Brexit); *see also* Sara Drake & Jo Hunt, *Clarifying the Duties of the UK Judiciary Post-Brexit:* Lipton and Anr *v* BA City Flyer Ltd, MOD. L. REV. (forthcoming 2022) (manuscript at 6–11) (elaborating).

135. *See In re* Facebook, Inc. Sec. Litig., 477 F. Supp. 3d 980, 993 n.2 (N.D. Cal. 2020); *see also In re* Nielsen Holdings PLC Sec. Litig., 510 F. Supp. 3d 217, 224 (S.D.N.Y. 2021).

interprets the GDPR's terms,[136] has confirmed that the GDPR applies to data processing by service providers in response to law enforcement or similar requests.[137] U.S. courts are already considering arguments that the GDPR acts as a blocking statute in civil discovery and in response to administrative subpoenas, with varying degrees of success.[138] Daskal has suggested that the GDPR may "yield[] new claims of conflict" by providers in response to SCA requests.[139] As Jessica Shurson explains, "experts tend to agree that [the] GDPR will almost always act as a blocking provision for routine SCA warrants."[140] U.S. law enforcement have repeatedly expressed concerns about the GDPR, fearing that it will ultimately diminish their access to data

136. *But see* EUWA, § 6(1) (UK) ("A [UK] court . . . is not bound by any principles laid down, or any decisions made, on or after [Brexit], by the European Court [of Justice] . . . ."); *see also id.* §§ 6(4)–(5B) (further exempting the UK Supreme Court and the Scottish High Court of Justiciary from being bound by "retained EU case law" in certain circumstances and allowing further exemptions to be regulated); The European Union (Withdrawal) Act 2018 (Relevant Court) (Retained EU Case Law) Regulations 2020, 2020/1525 (additionally exempting the Court of Appeal in England and Wales and certain higher courts); *see* Target Group Ltd v. Her Majesty's Revenue and Customs [2021] EWCA (Civ) 1043 [2021] STC 1662 [97] (suggesting that these only provide "power [to] the court[s] to depart from retained EU case law in . . . narrow circumstances").

137. *See* Case C-623/17, Priv. Int'l v. Sec'y of State for Foreign and Commonwealth Affs., 2020 E.C.R. 790. A separate EU instrument regulates data processing for law enforcement purposes by police and other "competent authorities." Directive 2016/680, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA (Law Enforcement Directive), 2016 O.J. (L 119) 89 [hereinafter LED]. *Priv. Int'l* confirms that where law enforcement request data from service providers, the GDPR will govern providers' data processing, rather than other instruments, such as the LED. *Priv. Int'l*, 2020 E.C.R. ¶47; *see* R (MR) v. Chief Constable of Sussex Police [2021] EWCA (Civ) 42 [35], [81] (confirming that data processing for law enforcement purposes by non-competent authorities, like service providers, is subject to the GDPR, not LED). As CLOUD Act agreements deal with data transfers from service providers to law enforcement, the GDPR rather than the LED is therefore the appropriate instrument to focus on.

138. *Compare, e.g.*, *In re* Avandia Mktg., Sales Pracs. & Prod. Liab. Litig., 484 F. Supp. 3d 249, 266–68 (E.D. Pa. 2020) (rejecting claim, holding "American law must take precedence"), *with In re* Hansainvest Hanseatische Inv.-GmbH, 364 F. Supp. 3d 243, 252 (S.D.N.Y. 2018) (granting application to compel disclosure from foreign custodians but requiring applicant to assume costs, "including the costs of compliance with the GDPR" and to "indemnify [foreign custodians] against any potential breaches of European data privacy laws"). *See* United States v. Fresenius Med. Care Holdings, Inc., No. 3:20-CV-00158, 2020 WL 3956647, at *8 (M.D. Tenn. July 6, 2020) (recording counsel argument that the GDPR justified a party's resistance to a DOJ administrative subpoena).

139. Jennifer Daskal, *Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0*, 71 STAN. L. REV. ONLINE 9, 12–13 (2018); *e.g.*, Brief for Respondent at 17, U.S. v. Microsoft Corp., 138 S. Ct. 118 (2018) (no. 17-2) (predicting that the GDPR would contribute to "international discord" for law enforcement seeking overseas data). *See generally* SOJ v. JAO [2019] EWHC (QB) 2569 [37.2] ("[T]he territorial reach of the GDPR is not in any event a matter of [U.S.] law.").

140. Jessica Shurson, *Data Protection and Law Enforcement Access to Digital Evidence: Resolving the Reciprocal Conflicts Between EU and US Law*, 28 INT'L J. L. & INFO. TECH. 167, 177 (2020).

for law enforcement investigations.[141] This risk appears credible. Providers, including global providers based in the United States, may well increasingly attempt to raise a comity defense in the face of SCA requests based on the GDPR.[142] Even if such defenses are rejected by U.S. courts, providers may ultimately prefer to face a contempt of court finding there than risk receiving an extensive fine for breaching the GDPR from one of its "supervisory authorities."[143]

The interplay between the GDPR and CLOUD Act agreements raises various challenging questions worthy of further investigation; indeed, ambiguity over how data protection law interacts with the U.S.-UK Agreement appears to be a driving force behind the continued delay by its parties to bring it into force.[144] First, is the United Kingdom's designation of the U.S.-UK Agreement actually able to remove UK law blocking statutes, including the UK GDPR? Achieving this is the United Kingdom's primary obligation under the U.S.-UK Agreement.[145] However, a recent judgment suggests that the United Kingdom's method of doing so—the section 52

141. *E.g.*, Downing, Germany speech, *supra* note 50 ("From our perspective, it seems that data protection laws are increasingly put forth as reasons for blocking the provision of essential information to third-party government law enforcement and regulatory agencies charged with assuring public safety and well-being."); *see* Matt Miner, Deputy Assistant Att'y Gen., U.S. Dep't of Just., Remarks at the American Bar Association Criminal Justice Section Third Global White Collar Crime Institute Conference (June 27, 2019), https://www.justice.gov/opa/speech/deputy-assistant-attorney-general-matt-min er-delivers-remarks-american-bar-association (remarking that "data privacy and other restrictions," including GDPR, "are an evolving area," "[f]urther complicating" law enforcement "access to electronic evidence"); Raman, *supra* note 3 (making similar remarks); David J. Redl, Assistant Sec'y of Com. for Commc'n and Info., Remarks at National Secretary Telecommunications Advisory Committee Meeting (May 17, 2018), https://www.ntia.doc.gov/ speech testimony/ 2018/remarks-assistant-secretary-redl-national-security-telecommunications-advisory (cautioning that these "create[] serious and unclear legal obligations" and risk a "widespread impact" on law enforcement and others); *see also* Downing, ELC speech, *supra* note 34.

142. *See supra* notes 139–140.

143. *See* GDPR, *supra* note 13, art. 83(5) (providing authority for supervisory authorities to impose administrative fines for GDPR infringements for improperly transferring data internationally reaching "up to 4 % of the total worldwide annual turnover of the preceding financial year . . . ."); *e.g.*, Vincent Manancourt, *With Amazon Fine, Luxembourg Emerges as Europe's Unlikely Privacy Champion*, POLITICO (July 30, 2021, 6:57 PM), https://www. politico. eu/ article/amazon-fine-luxembourg-europe-privacy-champion/ ("Amazon said [Luxembourg] had fined it a record €746 million after finding that the way the e-commerce giant handles people's personal information falls afoul of Europe's strict privacy code."). *See generally* GDPR, *supra* note 13, ch. VI (setting out the powers and functions of supervisory authorities).

144. *See* Commission Implementing Decision 2021/1773, 2021 O.J. (L 360) ¶¶ 153–56 (EU) (recording EU views of the U.S.-UK Agreement, as well as the United Kingdom's confirmation "that they will only let the [U.S.-UK] Agreement enter into force once they [have] . . . clarity with respect to compliance with the data protection standards for any data requested under [it].").

145. U.S. WHITE PAPER, *supra* note 9, at 4; UK EXPLANATORY MEMORANDUM, *supra* note 27, ¶¶ 7–8; Data Access Agreement Press Release, *supra* note 3; HL Deb (20 Nov. 2018) (794) cols. 139–40 (UK) (statement of Baroness Williams).

designation—may currently be ineffective. In *Open Rights Group*, the Court of Appeal of England and Wales stated that the "principle of supremacy of EU law" continues to apply to the "UK GDPR."[146] "If and to the extent that a domestic provision cannot be read in such a way as to comply with the [UK GDPR], it should be disapplied," the court held.[147] While this judgment has been criticized,[148] it may mean that the UK GDPR continues to have effect despite the section 52 designation purporting to make providers' conduct "lawful for all purposes." This invites a further question: assuming its current approach is ineffective, what can the United Kingdom do? At the time of writing, its proposed solution appears to be to repeal and replace the UK GDPR with a stand-alone UK data protection regime.[149] Whether the section 52 designation would override a new regime appears likely,[150] but is also not free from doubt.[151]

Taking into account EU law invites further questions. Even if the section 52 designation excused providers from complying with any

146. R (Open Rights Group) v. Sec'y of State for the Home Dep't [2021] EWCA (Civ) 800 [11]–[13]; *see* R (Open Rights Group) v. Sec'y of State for the Home Dep't) [2021] EWCA (Civ) 1573 [14]; *see also* Lipton v. BA City Flyer Ltd. [2021] EWCA (Civ) 454 [2021] 1 WLR 2545 [83] (providing "basic principles" for interpreting EU law within UK courts after Brexit). *See generally* European Union (Withdrawal) Act, 2018, c. 16, § 5(2) (UK) ("[T]he principle of supremacy of EU law continues to apply on or after [exit day] so far as relevant to the interpretation, disapplication or quashing of any enactment or rule of law passed or made before [exit day].").

147. *Open Rights Group* [2021] EWCA (Civ) 800 [11]. *See generally* R v. Sec'y of State for Transport, *ex parte* Factortame Ltd. [1991] AC 603 (HL) 658–59 (appeal taken from Eng.) (noting that, under then applicable EU law, "it has always been clear that it was the duty of a United Kingdom court, when delivering final judgment, to override any rule of national law found to be in conflict with any directly enforceable rule of [EU] law").

148. *E.g.*, Nicholas Kilford, *The Supremacy of Retained EU Law: 'We're Lost, But We're Making Good Time!'*, UK CONST. L. BLOG (July 27, 2021), https://ukconstitutionallaw.org/ 2021/07/27/nicholas-kilford-the- supremacy-of-retained-eu- law-were- lost- but- were- making- good- time/ (outlining "the ambiguity in the supremacy principle" and discussing "three problems" with *Open Rights Group* specifically).

149. Harry Yorke, *Oliver Dowden: Creating Our Own Data Laws Is One of Brexit's Best Prizes; Reformed Regulations Will Boost Our Digital Economy and Cut Pointless Red Tape*, TELEGRAPH (Aug. 25, 2021, 9:55 PM), https://www.telegraph.co.uk/politics/2021/08/25/oliver-dowden-creating-data-laws-one -b iggest-prizes-brexit/; *see* Press Release, UK Dep't for Digital, Culture, Media & Sport, UK Unveils Post-Brexit Global Data Plans to Boost Growth, Increase Trade and Improve Healthcare (Aug. 25, 2021), https://www.gov.uk/government/news/uk-unveils-post-brexit-global-data-plans-to-boost-growth-increase - trade-and-improve-healthcare ("Now that we have left the EU I'm determined to seize the opportunity by developing a world-leading data policy . . . It means reforming our own data laws so that they're based on common sense, not box-ticking.").

150. *See* European Union (Withdrawal) Act (EUWA) 2018, c. 16, § 5(1) (UK) ("The principle of the supremacy of EU law does not apply to any enactment or rule of law passed or made on or after [exit day].").

151. *See* JAY, *supra* note 133, § 3–038 ("[Ca]ses may still be decided in accord with retained EU law even if the law has subsequently been modified by UK law if in doing so [this] is consistent with the intention of the modification.") (citing EUWA, c. 16, § (6)(3)).

otherwise conflicting UK law obligations, could it excuse providers from obligations at EU law? As a directly applicable EU regulation, the EU GDPR applies across all EU member states, as well as the European Economic Area (EEA).[152] Many service providers operating in both the United States and United Kingdom also operate within the EU and EEA,[153] including in circumstances subjecting them to the requirements of EU law, such as the GDPR.[154] Given the EU law principle of supremacy, it appears that providers may remain subject to EU law conflicts regardless of the changes to data protection that are made at UK law. Again, if this is the case, what should be done? This question is of pressing importance. To meaningfully resolve conflicts between U.S. and EU law, an agreement between the United States and EU appears necessary.[155] Negotiating such an agreement to ensure its contents satisfy all relevant parties, including ultimately the CJEU, is, to say the least, difficult.[156] Indeed, related privacy and data protection concerns regarding the scope of the EU's own proposed "e-Evidence" direct access mechanism continue to stymie its progression.[157] Ultimately, resolution of these various UK and EU law questions appears necessary for the United States (or, indeed, the United Kingdom) to fully realize this private international law benefit of the U.S.-UK Agreement.

---

152. *See generally* GDPR, *supra* note 13, art. 3 (setting out its territorial scope). The application of the GDPR is not an "all or nothing" question; instead, providers must "assess[] whether particular processing. . . . falls within the scope of the [GDPR]." *See* EUROPEAN DATA PROTECTION BOARD, GUIDELINES 3/2018 ON THE TERRITORIAL SCOPE OF THE GDPR (ARTICLE 3) 4–5 (2019)*; e.g.*, Case C-507/17, Google v. Comm'r nationale de I'linformatique et des libertes, ECLI:EU:C:2019:772, ¶¶ 61–73 (Sept. 24, 2019) (holding that Google's obligations to "de-reference" data under the GDPR were territorially limited to "the Member States").

153. *See, e.g.*, Bala et al., *supra* note 128, at 6 ("AWS . . . has . . . regions in . . . France, Germany, . . . Sweden and [elsewhere].").

154. *See, e.g.*, Marco Stefan & Gloria González Fuster, *Cross-Border Access to Electronic Data Through Judicial Cooperation in Criminal Matters: State of the Art and Latest Development in the EU and US*, CTR. FOR EUR. POL'Y STUD. (Dec. 3, 2018), https://www.ceps.eu/ ceps- publications/ cross-border- access-electronic-data-through-judicial-cooperation-criminal-matters/ (discussing GDPR and its applicability to providers).

155. Thomas Streinz, *The Evolution of European Data Law*, *in* THE EVOLUTION OF EU LAW 902, 932 (Paul Craig & Gráinne de Búrca eds., 2021); *see* Shurson, *supra* note 140, at 181–82 (recognizing that service providers would be adversely impacted if the CLOUD Act were not reconciled with EU law); Abraha, *supra* note 51, at 149 (similar); *see also Joint US-EU Statement on Electronic Evidence Sharing Negotiations*, U.S. DEPT. OF JUST. (Sept. 26, 2019), https://www.justice.gov/ opa/ pr/joint -us- eu-statement- electronic-evidence-sharing-negotiations. *See generally supra* note 31 (detailing the ongoing EU-US negotiations arising from GDPR and related measures).

156. *See* Christakis & Terpan, *supra* note 31, at 104 (referring to these and related negotiations as "highly complex and challenging"); Downing, ELC speech, *supra* note 34 (discussing difficulties with U.S.-EU negotiations arising from GDPR and related measures).

157. *See, e.g.*, Stefan & Fuster, *supra* note 154, at 46–49 (outlining GDPR and related concerns with the proposed EU "e-Evidence" direct access mechanism)..

B. Public International Law: Extending Enforcement Jurisdiction

(1) How CLOUD Act Agreements Allow States To Expand Jurisdiction

A second significant benefit of CLOUD Act agreements is that they allow their members to expand jurisdiction internationally by lifting what is known as the prohibition against extraterritorial "enforcement jurisdiction" at international law. Enforcement jurisdiction "concerns the authority of a state to exercise its power to compel compliance with law."[158] U.S. and UK courts continue to recognize the continued force of this prohibition,[159] although there are growing debates as to whether and how it should apply to cross-border data flows.[160] It would traditionally prohibit U.S. or UK law enforcement from seeking to compel a foreign service provider not operating in their territory to disclose data under international law, as two seminal cases—one U.S. and one UK—from the 1980s bear out. In 1980, the D.C. Circuit Court of Appeals rejected an attempt by the Federal Trade Commission "to serve its investigatory subpoenas directly upon citizens of other countries by registered mail," holding that "the *act of service itself* constitutes an act of American sovereign power within the area of the foreign

158. RESTATEMENT (FOURTH) OF FOREIGN RELS. L. OF THE U.S. ch. 3, introductory note (AM. L. INST. 2018); *see* R (Jimenez) v. First Tier Tribunal [2019] EWCA (Civ) 51, [2019] 1 WLR 2956 [45] (Eng.) ("A state's enforcement jurisdiction includes its power to carry out its official functions if necessary by coercive means."); BOISTER, *supra* note 44, at 311 ("Activities requiring legal authority such as the gathering of admissible evidence. . . . are exercises in enforcement jurisdiction."); RESTATEMENT (FOURTH) OF FOREIGN RELS. L. OF THE U.S. § 432 cmt. A. ("A state typically exercises jurisdiction to enforce through its law-enforcement officers, often at the direction of its courts."). It is not engaged by law enforcement acts not backed by the possibility of sanction. *E.g.*, *Jimenez* [2019] EWCA (Civ) 51 [51]–[57]; *see* R (KBR, Inc.) v. Dir. of the Serious Fraud Off. [2021] UKSC 2, [2021] 2 WLR 335 [58]–[59] (appeal taken from Eng.) (UK). *See generally* Commodity Futures Trading Comm'n v. Nahas, 738 F.2d 487, 494 n.14 (D.C. Cir. 1984) ("The distinction between service of compulsory process and service of notice is critical under principles of international law due to the difference in judicial enforcement power that accompanies each.").

159. *E.g.*, Usoyan v. Rep. of Turkey, 6 F.4th 31, 39 (D.C. Cir. 2021) ("Turkey is a foreign power and—as Turkey itself concedes—its agents do not have the authority to perform law enforcement functions inside the United States.") (citing RESTATEMENT (FOURTH) OF THE FOREIGN RELS. L. OF THE U.S. § 432 cmt. B. ("[A] state may not exercise jurisdiction to enforce in the territory of another state.")); Perry v. Serious Organised Crime Agency [2012] UKSC 35, [2013] 1 AC 182 [94] (appeal taken from Eng.) (UK) (noting that exercising coercive jurisdiction extraterritorially "would be a particularly startling breach of international law"). *But see also KBR, Inc.* [2021] UKSC 2 [50]–[51] (following *Perry* but suggesting that "it may well be correct that not every case in which legislation confers powers to impose obligations on foreign persons abroad under pain of criminal sanction would necessarily constitute a breach of international law . . . .").

160. *See* LAW COMMISSION, *supra* note 59, ¶ 16.87 ("Strict adherence to the *Lotus*-based principle of enforcement jurisdiction is neither possible nor desirable when electronic data is sought."); *see also* CRAWFORD, *supra* note 92, at 462–64 (outlining the "present position" regarding enforcement jurisdiction); BOISTER, *supra* note 44, at 329–31 (discussing state attempts to unilaterally gather evidence extraterritorially, noting "the international legality of which may be dubious").

country's territorial sovereignty."[161] Enforcing such subpoenas "would clearly extend American enforcement jurisdiction beyond the limits of its prescriptive jurisdiction" under its empowering statute, and "violate[] a fundamental principle of international law."[162] Five years later, Hoffmann, J., (as he then was) in the Chancery Division of the High Court of England and Wales rejected a similar attempt to serve a subpoena on an American bank not party to the underlying proceedings.[163] He noted that subpoenas, requiring the production of documents backed by the threat of sanction, are "an exercise of sovereign authority"; as such, unilaterally requiring compliance by a foreign (United States) nonparty with a subpoena would be "an infringement of the sovereignty of the United States."[164] The U.S.-UK Agreement will, however, allow these authorities to be distinguished, expanding the ability of its members to assert extraterritorial jurisdiction over foreign service providers at international law.

This public international law benefit of direct access mechanisms flows from the nature of "jurisdiction" at international law. As in domestic law,[165] the term "jurisdiction" in international law is contextual and often confusing.[166] International law jurisdiction can be divided into several

161. F.T.C. v. Compagnie De Saint-Gobain-Pont-a-Mousson, 636 F.2d 1300, 1304 (D.C. Cir. 1980).

162. *Id.* at 1318; *see also id.* at 1316 ("When an American court orders enforcement of a subpoena requiring the production of documents and threatens noncompliance with that subpoena, it invokes the enforcement jurisdiction. . . .of the United States."); RESTATEMENT (FOURTH) OF FOREIGN RELS. L. OF THE U.S. § 432 reporters' notes 1 (referring to "executing an order for the production of documents" as an act "constituting jurisdiction to enforce"); *e.g.*, *In re* Search of Info. Associated with [redacted]@gmail.com, No. 16-MJ-00757, 2017 WL 3445634, at *14 (D.D.C. July 31, 2017) ("The SCA warrant was merely an exercise of this Court's enforcement jurisdiction").

163. Mackinnon v. Donaldson, Lufkin & Jenrette Sec. Corp. [1986] Ch 482, 493–95 (Eng.); *see* SAS Inst. Inc. v. World Programming Ltd. [2020] EWCA (Civ) 599 [68]–[70], *leave to appeal granted,* UKSC 2020/0118 (2021) (suggesting *Mackinnon* describes enforcement jurisdiction). *See* generally CRAWFORD, *supra* note 92, at 462 ("[O]rders for the production of documents may not be executed on the territory of another state, except under the terms of a treaty or other consent given."). Hoffman, J., would later serve as a Law Lord in the Judicial Committee of the House of Lords, now the UK Supreme Court.

164. *Mackinnon* [1986] EWHC (Ch) 482 at 494.

165. *See* Anisminic Ltd. v. Foreign Compensation Comm. [1968] 2 QB 862, 889 (Diplock LJ) (Eng.) ("'Jurisdiction' is an expression which is used in a variety of senses and takes its colour from its context."); United States v. L.A. Tucker Truck Lines, Inc., 344 U.S. 33, 39 (1952) (Frankfurter, J., dissenting) ("[T]he term 'jurisdiction'. . . is a verbal coat of too many colors."); *see, e.g.*, R (Priv. Int'l) v. Investigatory Powers Tribunal [2019] UKSC 22 (appeal taken from Eng.) (debating different interpretations of "jurisdiction" in a particular statute); *see also* United States v. Rodgers, 466 U.S. 475, 479–80 (1984). While "[d]omestic and international law on jurisdiction influence each other," they "are distinct bodies of law." RESTATEMENT (FOURTH) OF THE FOREIGN RELS. L. OF THE U.S. § 401 cmt. A; *e.g.* R (KBR, Inc.) v. Dir. of the Serious Fraud Off. [2021] UKSC 2, [2021] 2 WLR 33 [24]–[25] (appeal taken from Eng.) (UK) (noting uncertainty as to the "precisely defined rules in international law" regarding jurisdiction and therefore limiting an asserted extraterritorial act based on comity).

166. *See* R (Smith) v. Oxfordshire Assistance Deputy Coroner [2010] UKSC 29, [2011] 1 AC 1 [237] (Lord Collins) (Eng.) ("The expression 'jurisdiction' is used in many senses in international law.");

categories, including jurisdiction to prescribe, i.e. "to make law applicable to persons, property or conduct," and jurisdiction to enforce, i.e. "to exercise . . . power to compel compliance with law."[167] International law is often permissive concerning extraterritorial prescriptive jurisdiction.[168] In contrast, "[e]nforcement jurisdiction is strictly territorially bounded."[169] However, the prohibition against extraterritorial enforcement jurisdiction applies only to *unilateral* acts; where the foreign state of the territory concerned consents, no jurisdictional issue arises in respect of that foreign state under international law.[170] Foreign state consent may be provided

---

RESTATEMENT (FOURTH) OF THE FOREIGN RELS. L. OF THE U.S. § 401 ("The foreign relations law of the United States divides jurisdiction into three categories"); *e.g.*, R (Jimenez) v. First Tier Tribunal (Tax Chamber) [2019] EWCA (Civ) 51, [2019] 1 WLR 2956 [53] (appeal taken from Eng.) (UK) ("Delineating the precise boundary between prescriptive (or legislative) and enforcement jurisdiction in international law is far from straightforward."); *see F.T.C. v. Compagnie De Saint-Gobain-Pont-a-Mousson*, 636 F.2d at 1318 ("Questions of service of process, subject matter jurisdiction, and personal jurisdiction are invariably intertwined and, hence, frequently confused.").

167. RESTATEMENT (FOURTH) OF THE FOREIGN RELS. L. OF THE U.S. § 401; *see* CRAWFORD, *supra* note 92, at 440; *Smith*, [2010] UKSC 29 [241]–[43] (Lord Mance); *F.T.C. v. Compagnie De Saint-Gobain-Pont-a-Mousson*, 636 F.2d at 1315–17. The Restatement also includes jurisdiction to adjudicate, i.e. "to apply law to persons or things," as a third intermediary category. RESTATEMENT (FOURTH) OF THE FOREIGN RELS. L. OF THE U.S. § 401. The late Judge Crawford considered this an instance of enforcement jurisdiction, although conceded that at least aspects "may be better seen as a manifestation of prescriptive jurisdiction." CRAWFORD, *supra* note 92, at 440 n.3; *see* Alex Mills, *Rethinking Jurisdiction in International Law*, 84 BRIT. Y.B. INT'L. L. 187, 194–95 (2014) (summarising differing views). It is unnecessary to resolve this uncertainty in this article, as its focus is on enforcement jurisdiction.

168. *See* RESTATEMENT (FOURTH) OF THE FOREIGN RELS. L. OF THE U.S. §§ 401 cmt. B., 407 cmt. C., 422 n.1; Mills, *supra* note 167, at 195 ("The territorial character of enforcement jurisdiction is well established"); Robert J. Currie, *Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the Next Frontier?*, 53 CAN. Y.B. INT'L L. 63, 70 (2016) ("Extraterritorial *law-making* by states tends to be considered lawful [but]. . . [t]his generally permissive approach is in stark contrast to the rules surrounding the exercise *of enforcement jurisdiction*.") (emphasis added); *c.f.*, CRAWFORD, supra note 92, at 462 ("By contrast[with prescriptive jurisdiction], the unilateral and extraterritorial use of enforcement jurisdiction is impermissible.").

169. Currie, *supra* note 168, at 70; *see* S.S. Lotus (Fr. v. Turk.), Judgment, 1927 P.C.I.J. (ser. A) No. 10, at 18–19 (Sept. 7) ("[F]ailing the existence of a permissive rule to the contrary – [a state] may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial . . . ."); *see* Corfu Channel (UK v. Al.), Judgment, 1949 I.C.J. Rep. 4, 34–35 (Apr. 9) (rejecting the argument that the United Kingdom was entitled to unilaterally "secure possession of evidence in the territory of another State, in order to submit it to an international tribunal"); Michael Akehurst, *Jurisdiction in International Law*, 46 BRIT. Y.B. INT. L. 145, 146–48 (1972–1973) ("An act by one State in the territory of another State . . . for the *purpose* of enforcing the first State's . . . laws, is contrary to international law. . . [T]he act is a usurpation of the sovereign powers of the local State.").

170. RESTATEMENT (FOURTH) OF THE FOREIGN RELS. L. OF THE U.S. § 401 cmt. B ("The United States . . . generally exercises enforcement jurisdiction in the territory of another state only with the consent of the other state."); CRAWFORD, *supra* note 92, at 462 (referring to "treaty or other consent" as displacing this prohibition); *see* CAMPBELL MCLACHLAN, FOREIGN RELATIONS LAW 424 (2016) ("States may indeed by agreement between themselves abrogate the rule against the enforcement of foreign public law altogether."). *See generally* Compania Naviera Vascongado v. Steamship "Cristina" and Persons

through an international treaty—like the U.S.-UK Agreement[171]—or informally.[172] Through the U.S.-UK Agreement, the United States and United Kingdom have provided sufficient consent at international law to permit law enforcement from the other state to expand enforcement jurisdiction over service providers operating in their jurisdiction, through the lifting of "blocking statutes" that otherwise purport to make this unlawful under U.S. or UK law.[173] This is a potentially significant, arguably "sovereignty-enhancing," benefit.[174] However, an act may be lawful at international law, but unlawful under domestic law.[175] It is therefore necessary to turn to the law of each state to determine whether this benefit is realizable in practice.

The United Kingdom appears well-placed to reap this benefit—indeed, it expressly asserts the ability to do so, saying that the U.S.-UK Agreement will enable its law enforcement to compel data from providers previously "beyond the reach of existing domestic court orders" that could only be reached through MLA.[176] New UK legislation enacted specifically for the U.S.-UK Agreement, the Crime Overseas Production Orders Act 2019 (COPOA), permits court orders compelling stored data from foreign service

---

Claiming and Interest Therein [1938] AC (HL) 485, 496–97 (appeal taken from Eng.) (referring to territorial sovereignty as an "essential attribute" of "all sovereign independent States" but noting that States "have been led by courtesy as well as by self-interest to waive in favour of each other certain of their sovereign rights," including territorial sovereignty); Schooner Exch. v. McFaddon, 11 U.S. 116, 136 (1812) ("All exceptions. . .to the full and complete power of a nation within its own territories, must be traced up to the consent of the nation itself. They can flow from no other legitimate source.").

171. *See* Theodore Christakis & Kenneth Propp, *The Legal Nature of the UK-US CLOUD Agreement*, CROSS-BORDER DATA F. (Apr. 20, 2020), https:// www.crossborderdataforum.org/ the-legal-nature- of- the -u k- us- cloud- agreement/ (concluding that CLOUD Act agreements are "binding international agreement[s]" under international law).

172. RESTATEMENT (FOURTH) OF THE FOREIGN RELS. L. OF THE U.S. § 442 reporters' notes 3; CRAWFORD, *supra* note 92, at 462; *see* Bellia, *supra* note 107, at 80 ("[A] a state can simply give the searching state permission to examine data located within its territory."); *e.g.*, Reid v. Covert, 354 U.S. 1, 15 (1957) (referring to U.S. extraterritorial jurisdiction pursuant to a treaty); Casdagli v. Casdagli [1919] AC (HL) 145, 156 (appeal taken from Eng.) (UK) ("The jurisdiction exercised by His Majesty in Egypt is indeed extra-territorial, but it is exercised with the consent of the Egyptian Government . . . .").

173. *See supra* notes 56–57.

174. *Compare* Hannah L Buxbaum, *Transnational Regulatory Litigation*, 46 VIRG. J. INT'L L 252, 308 (2006) (arguing in the regulatory context that "if one theorizes sovereignty as status within the international community" then "bilateral cooperation instruments" can be described as "sovereignty-enhancing"), *with* NEW ZEALAND LAW COMMISSION AND MINISTRY OF JUSTICE, REVIEW OF THE SEARCH AND SURVEILLANCE ACT 2012: ISSUES PAPER NZLC IP40, ¶ 6.127 (Nov. 2016) "(A [CLOUD Act] agreement would . . . involve sacrificing a degree of sovereignty").

175. *See generally* F.T.C. v. Compagnie De Saint-Gobain-Pont-a-Mousson, 636 F.2d 1300, 1315 (D.C. Cir. 1980) ("[S]ome exercises of jurisdiction to which international law does not object may violate the Constitution or laws of the United States.").

176. Crime (Overseas Production Orders) Act (COPOA) 2019, c. 5, Explanatory Notes ¶¶ 1–4 (UK); *see id.* §§ 1(2), 1(4)–(5), 4(2) (providing for these powers).

providers operating in the United States, under threat of contempt of court,[177] even where these providers have no UK presence whatsoever.[178] Daskal describes this legislation as "a broad assertion of authority" but one "premised on consent," as requests must be channeled through the U.S.-UK Agreement (or any future similar arrangements with other foreign states).[179] Domestic UK law does not appear to meaningfully constrain the United Kingdom from making ample use of the U.S.-UK Agreement in this way. At UK law, two aspects of jurisdiction will normally be required in this context: "personal jurisdiction, i.e. who can be brought before the court, [and] subject matter jurisdiction, i.e. to what extent the court can claim to regulate the conduct of those persons."[180]

In the United Kingdom, personal jurisdiction is satisfied through service of process.[181] COPOA's service requirements "have been drafted to allow for flexibility,"[182] permitting overseas service in a wide range of scenarios, including electronically.[183] This requirement is therefore readily

177. Criminal Procedure Rules 2020, SI 2020/759, r. 47.68 (UK).

178. COPOA 2019, c. 5, §§ 4(2), (8)(a) (permitting orders against persons operating or based in a territory outside the United Kingdom where that territorial sovereign is party to a "designated international co-operation agreement" with the United Kingdom, "whether or not the person also creates, processes, communicates or stores data by electronic means in the United Kingdom"); *see* Ryan Junck et al., *What Recent US and UK Reforms to Information Sharing Mean for Cross-Border Investigations*, GLOB. INVESTIGATIONS REV. (July 18, 2019), https://globalinvestigationsreview.com/what-recent-us-and- uk-reforms-information-sharing-mean-cross-border-investigations ("The Crime (Overseas Production Orders) Act. . . empower[s] enforcement agencies to compel disclosure *from any individual or company operating or based abroad*, provided that the UK has a designated international cooperation agreement . . . with the country where the production order will be served.") (emphasis added).

179. Jennifer Daskal, *Transnational Government Hacking*, 10 J. NAT'L SEC. L. & POL'Y 677, 695 (2020); *see* COPOA 2019, c. 5, § 4(2) (requiring, among other criteria, that a court be satisfied that "there are reasonable grounds for believing that" the overseas service provider "against whom the order is sought" is "based in" or otherwise "operates in a country or territory outside the United Kingdom which is a party to, or participates in, the designated international co-operation arrangement.").

180. Société Eram Shipping Co. v. Cie Internationale de Navigation [2003] UKHL 30, [2004] 1 AC 260 [22]–[23] (quoting Mackinnon v. Donaldson, Lufkin & Jenrette Sec. Corp. [1986] Ch 482, 493 (Eng.)); SAS Inst. Inc. v. World Programming Ltd. [2020] EWCA (Civ) 599 [68]–[71], *leave to appeal granted* UKSC 2020/0118 (2021).

181. *Mackinnon* [1986] Ch 482, 493; *see* Stichting Shell Pensioenfonds v. Kyrs [2014] UKPC 41, [2015] AC 616 [27] (appeal taken from Virgin Is.) (UK) ("[T]o be amenable to its personal jurisdiction [a party] must be present within the jurisdiction or amenable to being served with the proceedings out of the jurisdiction, and he must have submitted voluntarily."). *See generally* DICEY, MORRIS & COLLINS ON THE CONFLICT OF LAWS ¶ 11-003 (Lord Collins of Mapesbury & Jonathan Harris eds., 15th ed. 2018) ("[I]n England service of process is the foundation of the court's jurisdiction to entertain a claim in personam . . . . [W]henever a defendant can be legally served with process, then the court, on service being effected, has jurisdiction to entertain a claim against him.").

182. HL Deb (10 Sept. 2018) (792) col. 196GC (UK) (statement of Baroness Williams); *id.* ("If a person is located outside the UK and the other conditions for granting a [COPOA] production order are fulfilled, a production order can be served.").

183. COPOA 2019, c. 5, §§ 9, 14, Explanatory Notes ¶ 52; Criminal Procedure Rules 2020, SI

established. Subject matter jurisdiction may be more difficult: under UK law, the extraterritorial scope (if any) of a statute "is a matter of subject matter jurisdiction."[184] A statute's extraterritorial subject matter may be express or implied.[185] Where the legislature has "provided expressly for [a statute's] extraterritorial application," as the U.S. Congress did with the CLOUD Act and the UK Parliament has with COPOA,[186] UK courts will give effect to that intent—even if inconsistent with international law.[187] UK courts normally apply a "presumption against extraterritoriality," limiting a statute's extraterritoriality to avoid infringing the sovereignty of foreign states and due to broader comity concerns.[188] The House of Lords has held that "[w]here, however, Parliament incorporates into domestic legislation an international [agreement] which necessarily gives to that domestic legislation extraterritorial effect in the broadest sense an entirely different

2020/759, r. 47.68(4) (UK); U.S.-UK AGREEMENT, *supra* note 2, arts. 5(5), 10(2); *see also* COPOA 2019, c. 5, § 14(4)(d)(i) (further permitting overseas service "in accordance with arrangements made . . . by the Secretary of State"); U.S.-UK AGREEMENT, *supra* note 2, arts. 6(2), 10(6). Stricter requirements as to service in civil proceedings are irrelevant. *See, e.g.*, R (KBR, Inc.) v. Dir. Of the Sec. Fraud Off. [2018] EWHC (Admin) 2368, [2019] QB 675 [99(i)], *overruled on other grounds by* [2021] UKSC 2, [2021] 2 WLR 335 (UK) (referring to the applicant's reliance on civil procedure rules as "the central fallacy" in its personal jurisdiction argument, noting that "those provisions are irrelevant" to the analogous criminal disclosure powers it was evaluating).

184. *KBR* [2018] EWHC (Admin) 2368 [72(i)], *aff'd on this point,* [2021] UKSC 2 [59] (UK); *see* Masri v. Consolidated Contractors Int'l. Co. [2008] EWCA (Civ) 303, [2009] QB 45 [30] (UK) ("Subject matter jurisdiction is concerned, inter alia, with the extent to which the law . . . applies extra-territoriality."). *See generally* Jetivia SA v. Bilta Ltd. [2015] UKSC 23, [2016] 1 AC 1 [212] (appeal taken from Eng.) (UK) ("Whether a court has . . . subject matter jurisdiction is a question of the construction of the relevant statute.").

185. *KBR* [2021] UKSC 2 [28]–[29]; DAVID FELDMAN, DIGGORY BAILEY & LUKE NORBURY, BENNION, BAILEY, AND NORBURY ON STATUTORY INTERPRETATION § 6.10 (8th ed. 2020).

186. *KBR* [2018] EWHC (Admin) 2368 [61]; *see supra* text accompanying notes 176–178.

187. *E.g.*, Assange v. Swed. Prosecution Auth. [2012] UKSC 22, [2012] 2 AC 471(appeal taken from Eng.) (UK) (holding that if the proper interpretation of a particular UK statute gave rise to a "possible or likely discrepancy [with] the United Kingdom's international obligations . . . that is in no way impermissible . . . . It is the consequence of the United Kingdom's dualist system [and] of Parliamentary sovereignty . . . ."). *See generally* R (Miller) v. Sec'y of State for Exiting the Eur. Union [2017] UKSC 5, [2018] AC 61 [56], [167], [244] (appeal taken from Eng.) (UK) (affirming Parliamentary Sovereignty and the United Kingdom's dualist approach to international law).

188. *KBR*, [2021] UKSC 2 [27]–[32]; *see id.* at [28] ("The more exorbitant the jurisdiction, the more is likely to be required of the statutory provisions in order to rebut the presumption against extra-territorial effect."); Masri v. Consol. Contractors Int'l. Co. SAL [2008] EWCA (Civ) 303, [2009] QB 450 [38]–[39] (Eng.) (noting that UK courts may limit extraterritorial jurisdiction over third parties subject to personal jurisdiction, due to "concerns relating to international comity"); Mackinnon v. Donaldson, Lufkin & Jenrette Sec. Corp. [1986] Ch 482, 494 (Eng.) (recognizing "[t]he need to exercise the court's jurisdiction with due regard to the sovereignty of others")); *see also* Société Eram Shipping Co. v. Cie Internationale de Navigation [2003] UKHL 30, [2004] 1 AC 260 [67] (appeal taken from Eng.) (UK) (following *Mackinnon* on this point).

situation arises."[189] Then, "the basis for the presumption no longer exists."[190] Here, similarly, there is no need to limit extraterritorial jurisdiction to avoid infringing U.S. sovereignty, given the U.S.-UK Agreement evidences the United States' consent for such extraterritoriality.[191] As these jurisdictional requirements are met, the United Kingdom therefore appears to have significant scope to use the U.S.-UK Agreement to expand its jurisdiction over foreign service providers.

UK courts may nonetheless constrain the extraterritorial reach of the United Kingdom's new COPOA/U.S.-UK Agreement powers to comply with the prohibition against extraterritorial enforcement jurisdiction or to avoid related conflicts or comity concerns. It is beyond the scope of this article to comprehensively address the continued state of this prohibition or how it should be applied in today's digital world—although these are pressing tasks for scholars.[192] It is, however, arguable that whether a state has sufficient "consent" in this context is a multifactorial rather than binary question.[193] The "un-territorial" nature of electronic data renders it particularly vulnerable to sovereignty claims by "overlapping jurisdictions."[194] The fact that UK law enforcement have the consent of the United States to serve an extraterritorial request for data on service providers based in the United States may merely be necessary but not sufficient at international law; other (non-consenting) states may have legitimate sovereignty claims over that provider and/or the requested data.[195] Consider, for example, that UK law enforcement are expected to direct the bulk of their U.S.-UK Agreement requests to global service providers.[196] As noted, such

189. Holmes v. Bangl. Biman Corp. [1989] 1 AC (HL) 1112, 1148 (Lord Jauncey) (appeal taken from Eng.); *see also id.* at 1132–38 (Lord Griffiths and Lord Bridges arriving at the same conclusion pronounced by Lord Jauncey).

190. *Id.* at 1148.

191. *See id.* at 1137–38 ("In such circumstances our domestic legislation is not an interference with the sovereignty of other countries but the recognition of their wish that we should alter our law to accord with the common will.").

192. *See supra* note 160.

193. *See* Asaf Lubin, *The Prohibition on Extraterritorial Enforcement Jurisdiction in Cyberspace*, *in* ELGAR RESEARCH HANDBOOK ON EXTRATERRITORIALITY AND INTERNATIONAL LAW 4–6 (Austen L. Parrish & Cedric Ryngaert eds., 2022 forthcoming), https:// papers.ssrn. com/sol3/ papers.cfm? abstract_id=4012007 (proposing a multifactorial test for resolving competing claims over data in cyberspace).

194. Anke Sophie Obendiek, *What Are We Actually Talking About? Conceptualizing Data as a Governable Object in Overlapping Jurisdictions*, INT'L STUD. Q. (2021 forthcoming); Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L. J. 326 (2015).

195. *See* Lubin*, supra* note 193, at 4–6.

196. *See, e.g.*, HC Deb (30 Jan. 2019) (653) cols. 859–60 (statement of Minister Wallace) ("This legislation [COPOA] is about the data predominantly held by Facebook and Google and everything else . . . .").

providers operate in multiple jurisdictions, often in circumstances subjecting them to data protection regimes like the GDPR.[197] Data protected by the GDPR, such as the Facebook messages of a French national, may well need to be processed by Facebook to comply with a request by UK law enforcement under the U.S.-UK Agreement.[198] While the status of the prohibition against extraterritorial enforcement jurisdiction requires further consideration, were a UK court to become aware of this potential French or EU sovereignty concern, it may ultimately "read down" the subject matter jurisdiction of COPOA on (linked) common law grounds in any event, to avoid infringing foreign nations' sovereignty, or for related comity concerns.[199] This is most likely to occur where compliance with a UK COPOA order would require the responding service provider to breach foreign law.[200] Separately, it also remains debatable whether a UK court would interpret COPOA as properly permitting orders to be issued to U.S. service providers with no UK connections whatsoever.[201] In other contexts, UK courts have read down apparently unlimited extraterritorial jurisdiction over foreign persons by requiring that such persons have a "sufficient connection" to the United Kingdom.[202] Such an interpretation may also be

197. *See supra* notes 153–154.

198. This may happen inadvertently, when UK law enforcement seek, for example, Facebook messages of a UK national communicating with a French national. Additionally, the U.S.-UK Agreement permits each state to directly target data of any third country national in any event. *See* U.S.-UK AGREEMENT, *supra* note 2, art. 5(10) (providing certain default obligations when third country national data is targeted).

199. *See* R (KBR, Inc.) v. Dir. of the Serious Fraud Off. [2021] UKSC 2, [2021] 2 WLR 335 [24]–[25] (appeal taken from Eng.) (UK).

200. Bank Mellat v. HM Treasury [2019] EWCA (Civ) 499 [63(iii)] (Eng.) ("An order will not lightly be made where compliance would entail a party to English litigation breaching its own (i.e., foreign) criminal law, not least with considerations of comity in mind."); Masri v. Consol. Contractors Int'l. Co. SAL [2008] EWCA (Civ) 303, [2009] QB 450 [47] (Eng.) ("[I]t would be an exorbitant exercise of jurisdiction to put a third party abroad in the position of having to choose between being in contempt of an English court and having to dishonour its obligations under a [foreign] law which does not regard the English order as a valid excuse."). *But see Bank Mellat* [2019] EWCA (Civ) 449 [63(i)] ("[T]he English Court[] has jurisdiction to order production and inspection of documents, regardless of the fact that compliance with the order would or might entail a breach of foreign criminal law in the 'home' country of the party the subject of the order."); *e.g.*, Owners of the Motor Vessel 'Gravity Highway' v. Owners of the Motor Vessel 'Maritime Maisie' [2020] EWHC (Comm) 1697 [50]–[52] (Eng.) (rejecting a party's attempt to withhold disclosure on the basis this would "place them in breach of Korean data protection regulations").

201. *Cf.* Crime (Overseas Production Orders) Act (COPOA) 2019, c. 5 (UK). Most, but not all, of COPOA's service methods are for overseas providers with at least some UK operations. *See supra* note 183; *e.g.*, COPOA 2019, c. 5, Explanatory Notes ¶ 52 ("Where a person has no principal office in the UK, documents can also be served at any place in the UK where that person carries on business or conducts business activities.").

202. *E.g.*, *Masri* [2008] EWCA (Civ) 303 [36]. These are however often based at least in part on sovereignty concerns which, here, may not arise. *Id.* at [59].

appropriate to give effect to the recipient service providers' own "due process" rights under Article 6(1) of the ECHR,[203] although historically this right appears to have had little impact in this context.[204]

(2) "Expanding Jurisdiction" Over UK Service Providers Would Also Significantly Benefit U.S. Law Enforcement—If Permitted Under The Due Process Clause

Just as the United States should be considered motivated to use the U.S.-UK Agreement to minimize conflicts,[205] it has credible reasons to want to use direct access mechanisms for this second benefit, i.e. expanding jurisdiction over foreign service providers. Cybercrime investigations—into crimes which "know no borders," operated through "complex criminal networks . . . across the world[206]—are of growing importance for U.S. law enforcement.[207] They are thus likely to be particularly tempted to seek to use CLOUD Act agreements to exercise expanded jurisdiction against service providers harboring cybercrimnal data overseas. Indeed, U.S law enforcement appear to have a significant appetite for data currently available only through MLA and related cooperative mechanisms. Reported examples—potentially representative of a much large number of analogous criminal investigations—show that in the past few years alone U.S. law enforcement have used MLA to obtain subscriber information, chat logs, and other data on targets' email, ISP, and social media accounts,[208] as well as to

203. ECHR, art. 6(1) (relevantly providing that, "[i]n the determination of his civil rights and obligations . . . everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law").

204. Ralf Michaels, *Jurisdiction, Foundations*, *in* ELGAR ENCYCLOPEDIA OF PRIVATE INTERNATIONAL LAW J.2 (Jürgen Basedow et al. eds., 2017) (noting that "due process and fair trial rights" under Article 6(1) of the ECHR "could be viewed as limiting the exercise as jurisdiction" but "[i]n reality" these and related laws "ha[ve] played a fairly limited role in limiting jurisdiction"). The ECtHR has found violations of due process under Article 6(1) of the ECHR where national courts "hav[e] overstepped the limits of [their] jurisdiction." *E.g.*, Sokurenko and Strygun v. Ukraine, App. No. 29458/04, ¶¶ 24–28 (ECtHR, July 20, 2006). However, it appears that the extent of such jurisdiction is treated purely as a matter of domestic law, leaving states free to assert broad extraterritorial authority. *See generally id.* ¶ 116 ("[I]t is for the national authorities, notably the courts, to interpret and apply domestic law.").

205. *See supra* Part III.A(2).

206. *Cybercrime*, INTERPOL (last accessed Nov. 18, 2021), https://www.interpol.int/ Crimes/ Cyb ercrime.

207. U.S. Dep't of Justice, Report of the Attorney-General's Cyber Digital Task Force xi (2018) ("Cyber-enabled attacks are exacting an enormous toll on American businesses, government agencies, and families"); *see* Steve Morgan, *Cybercrime To Cost the World $10.5 Trillion Annually by 2025*, CYBERCRIME MAG. (Nov. 13, 2020), https://cybersecurityventures.com /cybercrime-damages-6-trillion-by- 2021/ (noting that "[c]ybercrime has [already] hit the U.S. so hard").

208. United States v. Killen, 729 F. App'x 703, 714 n.7 (11th Cir. 2018) (relying on business records, created for purpose of organization's administration and consisting of "transactional and identifying information, such as chat logs . . . ; photographs . . . ; bind logs . . . ; and identifying account information"

wiretap their electronic communications.[209] The Mueller Inquiry alone "made 13 requests to foreign governments pursuant to [MLA],"[210] including (at least) one to the UK for electronic and other documents that was tied up in court for over 15 months.[211] A separate MLA request from the United States for information UK law enforcement had gathered about suspected terrorists operating in Syria recently took more than five years for UK courts to resolve due to concerns that the United States would seek to use information transmitted in criminal proceedings for which the death penalty may be imposed.[212] While that timeframe may be particularly egregious, MLA is commonly perceived to be slow and cumbersome.[213] In contrast, the United Kingdom has given overseas service providers a default period of seven days to respond to its U.S.-UK Agreement requests and anticipates the entire evidence-gathering process under COPOA will take "60 days or perhaps less."[214] Were the United States to set similar requirements on UK service providers responding to U.S-UK Agreement requests,[215] U.S. law enforcement could therefore more swiftly obtain data from UK service providers through this method when an opportunity arises, rather than through MLA,[216] including for criminal investigations that may ultimately

to obtain information); State *ex rel.* Okla. Bar Ass'n v. Ezell, 2020 OK 55 ¶ 7, 466 P.3d 551, 553–54 (Okla. Sup. Ct. 2020) (relying on emails sent to obtain requisite information); United States v. Nikulin, No. CR 16-00440 WHA, 2020 WL 5847518, at *3 (N.D. Cal. Oct. 1, 2020) (noting that defendant's mental health and medical records, defendant's email exchanges with friends and family, and defendant's phone call transcripts were all reviewed).

209. United States v. Loera, 333 F. Supp. 3d 172, 180 (S.D.N.Y. 2018).

210. ROBERT S. MUELLER, III, REPORT ON THE INVESTIGATION INTO RUSSIAN INTERFERENCE IN THE 2016 PRESIDENTIAL ELECTION 13 (2019).

211. R (Terra Servs. Ltd.) v. Nat'l Crime Agency [2020] EWHC (Admin) 1640, [2021] 1 WLR 1 [2] (Eng.); *see also* R (Terra Servs. Ltd.) v. Nat'l Crime Agency [2019] EWHC (Admin) 1933 [3] (Eng.) (noting that this litigation arose from an MLA request from the Mueller Inquiry).

212. Elgizouli v. Sec'y of State for the Home Dep't [2020] UKSC 10 [16]–[61], [2020] 2 WLR 857 (appeal taken from Eng.); R (Elgizouli) v. Sec'y of State for the Home Dep't [2020] EWHC (Admin) 2516 (Eng.).

213. *See, e.g.*, CLARKE ET AL., *supra* note 47, at 226–27. *See also* Data Access Agreement Press Release, *supra* note 3.

214. COPOA 2019, c. 5, § 5(5); HOME OFF., *supra* note 2, at 7 (UK); *see* Ryan Junck et al., *supra* note 178 (referring to the decreased timeframe as "[p]erhaps the most significant aspect of [COPOA]").

215. The U.S.-UK Agreement contemplates its members imposing "arrangements" and "requirements as to the manner" data is transmitted and produced from service providers. *See* U.S.-UK AGREEMENT, *supra* note 2, arts. 6(2), 6(4), 10(6), 10(11). These powers may possibly be used to set time-frames.

216. *See, e.g.*, CLARKE ET AL., *supra* note 47, at 226–27.

result in death penalty proceedings[217]—thus avoiding the extended delays the United States has recently experienced during MLA.[218]

It is appropriate to acknowledge that, at present, this public international law benefit may not be as apparent for the United States as it is for the United Kingdom. Far more service providers from which criminal evidence is commonly sought are currently U.S.—rather than UK—based.[219] Thanks to this, as well as the broad extraterritorial scope of the SCA and similar U.S. criminal investigatory and national security powers,[220] U.S. law enforcement can therefore readily obtain vast volumes of data for criminal investigations with relative ease without recourse to international arrangements. Looking ahead, however, the domination of U.S. service providers may be lessening. There are some indications that consumer demand for increased privacy protections, both within and outside the United States,[221] coupled with the continued failure of Congress to enact a comprehensive data protection law,[222] will cause a consumer shift to non-

217. Tim Cochrane, *The Impact of the CLOUD Act Regime on the UK's Death Penalty Assurances Policy*, U.K. CONST. L. BLOG (June 1, 2020), https:// ukconstitutionallaw.org/ 2020/06/01/tim-cochrane-the- impact- of- the- cloud -act- regime-on- the- uks- death- penalty- assurances- policy/; *see* U.S.-UK AGREEMENT, *supra* note 2, art. 8(4)(a).

218. *See infra* notes 211–213.

219. *See* Woods, *supra* note 42, at 621–22.

220. *See supra* note 42 (discussing the broad extraterritorial scope of the SCA): *e.g.*, *infra* notes 319–320 (Wiretap Act). In certain contexts, U.S, law enforcement may also obtain criminal evidence using extensive extraterritorial national security powers. *See, e.g.*, The Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 *et seq.* [hereinafter FISA]; United States v. Turner, 840 F.3d 336, 341 (7th Cir. 2016) (citing 18 U.S.C. § 1806(c)) ("[W]hile the government must have a measurable foreign intelligence purpose, other than just criminal prosecution, the amended FISA statute does not oblige the government to demonstrate to the FISA court that its primary purpose in conducting electronic surveillance is *not* criminal prosecution.") (citation and quote marks omitted). *But see, e.g.*, Asha Rangappa, *It Ain't Easy Getting a FISA Warrant: I Was an FBI Agent and Should Know*, JUST SEC. (Mar. 6, 2017), https:// www. justsecurity. org/38422/aint-easy-fisa- warrant- fbi-agent/ (arguing that the use of FISA powers for criminal investigations is difficult).

221. *See* CONSUMERS INTERNATIONAL AND INTERNET SOCIETY, THE TRUST OPPORTUNITY: EXPLORING CONSUMERS' ATTITUDES TO THE INTERNET OF THINGS 1, 3 (2019), https:// www. internetsociety. org/wp-content/uploads/2019/05/CI_IS_Joint_Report-EN.pdf (surveying "consumers in Australia, Canada, France, Japan, UK and the US" and concluding that, "[g]iven the level of concern amongst owners and non-owners, there is potential for companies to use high levels of privacy and security as a way to stand out from the crowd and build trust with current and future customers"); PEW RSCH. CTR., AMERICANS AND PRIVACY: CONCERNED, CONFUSED AND FEELING LACK OF CONTROL OVER THEIR PERSONAL INFORMATION 15 (2019), https://www.pewresearch.org/ internet/2019/11/15/ americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-infor matio n/ ("Seven-in-ten Americans say they feel as if their data is less secure today than it was five years ago").

222. *See* Opinion*, Congress Should Act on Privacy, Rather Than Leaving the Job to Regulators*, WASH. POST (Sept. 30, 2021, 2:52PM), https://www.washingtonpost.com/opinions/2021/09/30/congress-should- act-privacy-rather-than-leaving-job-regulators/; Jessica Rich, *After 20 Years of Debate, It's Time for Congress to Finally Pass a Baseline Privacy Law*, BROOKINGS (Jan. 14, 2021), https:// www. brookings.edu/blog/techtank/2021/01/14/after-20-years-of-debate-its-time-for-congress-to-finally- pass-

U.S. based providers claiming to be beyond the reach of U.S. law.[223] Although it is likely too soon to speak of the imminent demise of U.S. service providers' global domination, U.S. law enforcement should not be complacent. Indeed, an ongoing DOJ Inspector-General Audit indicates they are not; this states that the Office of International Affairs (OIA) within DOJ "will need to allocate resources, including attorneys and support personnel to carry out [its new issuing] role" under CLOUD Act agreements.[224] As the OIA will have responsibility only for *outgoing* U.S. requests under CLOUD Act agreements, not *incoming* foreign requests,[225] this is compelling evidence that, despite the United States' public statements suggesting otherwise,[226] it anticipates making ample use of the U.S.-UK Agreement and similar future agreements, for one or both of the two benefits this Part III has outlined so far.

Assuming then that the United States is *motivated* to use CLOUD Act agreements to expand jurisdiction over foreign providers in the manner outlined, a further question remains whether it is *capable* of doing so under U.S. law. On this point, the United Kingdom's interpretation of the U.S.-UK Agreement as allowing it to expand jurisdiction extraterritorially should guide the United States' own interpretation of this agreement under U.S. law.[227] Indeed, at first glance, the U.S. jurisdictional issues appear similar to those in the United Kingdom: "A court must have the power to decide the claim before it (subject-matter jurisdiction) and power over the parties before

---

a-baseline-privacy-law/.

223. *E.g.*, *10 Reasons to Choose Mailo Pro for Your Business or Organization*, MAILO BLOG (Apr. 15, 2021), https://blog.mailo.com/ blog/en/10-reasons-to-choose-mailo-pro.htm ("[T]he data is securely hosted in France and is not subject to the American CLOUD Act[.]"); *Northern Data Closes Acquisition of Data Center Site in Northern Sweden and Continues Successful Expansion Driven by Enormous Demand*, BUSINESS WIRE (Mar. 8, 2021), https://www.businesswire.com/news/ home/20210308005295/ en/ Northern-Data-closes-acquisition-of-data-center-site-in-Northern-Sweden-and-continues-successful-expansion-driven-by-enormous-demand ("As a European company, we are not subject to the U.S. Cloud Act[.]"); *see, e.g.*, Anthony Cuthbertson, *Whatsapp Sees Sudden Drop in Downloads as Millions Turn to Telegram and Signal*, INDEPENDENT (Jan. 15 ,2021), https://www.independent.co.uk/life-style/gadgets-and -tech/whatsapp-privacy-update-signal-telegram-b1787831.html. While WhatsApp is a U.S. service provider, Telegram is formally not.

224. DOJ IG AUDIT, *supra* note 71, at 19.

225. AG Order No. 4877-2020, 85 Fed. Reg. 67446-01 (Oct. 23, 2020) (to be codified at 28 C.F.R. § 0.64–6); *see* U.S.-U.K. AGREEMENT, *supra* note 2, arts. 1(8), 5(5)–(12).

226. *See supra* text accompanying notes 68–83.

227. *See* Water Splash, Inc. v. Menon, 137 S. Ct. 1504, 1512 (2017) ("[T]his Court has given considerable weight to the views of other parties to a treaty.") (internal quotation marks and citations omitted). UK law takes a similar approach. *See, e.g.*, T v. Sec'y of State for the Home Dep't [1996] AC 742 (HL) 779 (Lord Lloyd) (appeal taken from Eng.) (UK) ("In a case concerning an international convention it is obviously desirable that decisions in different jurisdictions should, so far possible, be kept in line with each other.").

it (personal jurisdiction) before it can resolve a case."[228] The relative significance of these two jurisdictional requirements is, however, inverse in the United States. "Subject matter jurisdiction" to issue an SCA order appears straightforward:[229] it is established where the court has subject matter jurisdiction over the underlying offense being investigated.[230] Assuming the SCA order is sought to investigate U.S. criminal offenses—over which federal courts have jurisdiction[231]—subject matter jurisdiction should therefore arise. Unlike in the United Kingdom, in the United States, the territorial reach of the SCA is not a question of subject matter jurisdiction.[232] Nonetheless, while not a jurisdictional issue in that narrow sense,[233] Daskal's argument about the (lack of) extraterritorial reach of the SCA or CLOUD Act has practical significance and is addressed below.[234]

Personal jurisdiction is a different story. It is widely accepted that "[a] federal court will enforce an investigative subpoena issued to a foreign national when it has personal jurisdiction over the subpoenaed party."[235] The Supreme Court recently affirmed that "[t]he canonical decision in this area remains *International Shoe*."[236] This held that personal jurisdiction

228. Lightfoot v. Cendant Mortg. Corp., 137 S. Ct 553, 562 (2017).

229. *See generally* Ruhrgas AG v. Marathon Oil Co., 526 U.S. 574, 587 (1999) ("[I]n most instances subject-matter jurisdiction will involve no arduous inquiry.").

230. *See* 18 U.S.C. §§ 2703(a), (b)(1)(A), (c)(1)(A), 3(d) (providing that SCA orders may be issued by any "court of competent jurisdiction"); 18 U.S.C. § 2711(3)(A)(i) (defining this term in part to mean "any district court of the United States that . . . has jurisdiction over the offense being investigated"); *e.g.*, United States v. Hopkins, No. 19-10135-EFM, 2020 WL 5642354, at *1–2 (D. Kan. Sept. 22, 2020); U.S. v. Rogers, No. 18-10018-EFM, 2019 WL 339590, at *6 (D. Kan. Jan. 28, 2019); United States v. Shultz, No. 16-10107-01-EFM, 2018 WL 534333, at *7 (D. Kan. Jan. 24, 2018); United States v. Search of Info. Associated with Fifteen Email Addresses, No. 2:17-CM-3152-WC, 2017 WL 4322826, at *3 (M.D. Ala. Sept. 28, 2017), *on reconsideration sub nom*. United States v. Search of Info. Associated with Fifteen Email Addresses, No. 2:17-CM-3152-WKW, 2017 WL 8751915 (M.D. Ala. Dec. 1, 2017). *See generally* United States Cath. Conf. v. Abortion Rts. Mobilization, Inc., 487 U.S. 72, 76 (1988) (noting, in the civil context, that "if a district court does not have subject-matter jurisdiction over the underlying action, and the process was not issued in aid of determining that jurisdiction, then the process is void").

231. *See* United States v. Williams, 341 U.S. 58, 65 (1951) ("The District Court ha[s] jurisdiction of offenses against the laws of the United States.") (citing 18 U.S.C. § 3231).

232. *See* Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247, 253–54 (2010) (rejecting the argument that "the extraterritorial reach of [a statute] raise[s] a question of subject-matter jurisdiction"); *id.* at 254 ("[T]o ask what conduct [the statute] reaches is to ask what conduct [it] prohibits, which is a merits question. Subject-matter jurisdiction, by contrast, refers to a tribunal's power to hear a case.") (internal quotation marks and citations omitted).

233. *See* Henderson *ex rel.* Henderson v. Shinseki, 562 U.S. 428, 435 (2011) ("We have urged that a rule should not be referred to as jurisdictional unless it governs a court's . . . subject-matter or personal jurisdiction.").

234. *See supra* text accompanying notes 89–90; *infra* Part IV.B(2).

235. *E.g.*, Silverman v. Berkson, 141 N.J. 412, 423 (1995) (citing *In re* Sealed Case, 832 F.3d 1268, 1262 (D.D.C. Cir. 1987), *abrogated on other grounds by* Braswell v. United States, 487 U.S. 99 (1988)).

236. Ford Motor Co. v. Mont. Eighth Jud. Dist. Ct., 141 S. Ct. 1017, 1024 (2021) (citing Int'l Shoe

ordinarily requires two findings:[237] first, that the nonresident party has "certain minimum contacts" with the forum;[238] and, secondly, that asserting jurisdiction over the party would be "reasonable in the circumstances."[239] While typically "the issue of minimum contacts does not arise in criminal cases"[240]—the physical presence of a criminal defendant before a court may establish personal jurisdiction[241]—courts apply the civil minimum contacts standard when asked to issue subpoenas and similar instruments to disinterested third parties like service providers during criminal investigations.[242] The United States' position, set out in its *White Paper*, is that "personal jurisdiction" constraints deny U.S. law enforcement the ability to use the U.S.-UK Agreement to expand enforcement jurisdiction at public international law. The focus of the remaining Part IV of this article evaluates this position.

Co. v. Washington, 326 U.S. 310, 316 (1945)).

237. Personal jurisdiction can be further divided into "two types . . . : 'general' (sometimes called 'all-purpose') jurisdiction and 'specific' (sometimes called 'case-linked') jurisdiction." Bristol-Myers Squibb Co. v. Superior Ct. of Cal., 137 S. Ct 1773, 1780 (2017). General jurisdiction arises "only where a defendant is 'essentially at home' in the [forum]," and is therefore presumably inapplicable here. *Ford Motor Co.*, 141 S. Ct. at 1024 (citing Goodyear Dunlop Tires Operations, S.A. v. Brown, 564 U.S. 915, 919 (2011)).

238. *Bristol-Myers Squibb*, 137 S. Ct at 1785–86 (citations omitted). This first factor is often divided into two parts. *Id.* ("First, the defendant must have purposefully availed itself of the privilege of conducting activities within the forum State or have purposefully directed its conduct [there]. Second, the plaintiff's claim must "'[A]rise out of or relate to" the defendant's forum conduct.") (quotation marks and citations omitted). For this article's purposes, however, it is sufficient to refer generally to the "contacts" requirement. *See, e.g.*, RESTATEMENT (FOURTH) OF FOREIGN RELS. L. § 422, Cmt. a (AM. L. INST. 2018) (referring generically to "the contacts prong" of "[t]he due-process analysis"); *see also Ford Motor Co*., 141 S. Ct. at 1033 (Alito, J., concurring) ("[A]rise out of' and 'relate to' overlap and are not really two discrete grounds for jurisdiction.").

239. *Bristol-Myers Squibb*, 137 S. Ct. at 1786 (citations omitted).

240. United States v. Bodmer, 342 F. Supp. 2d 176, 188 (S.D.N.Y. 2004).

241. *E.g.*, United States v. Rendon, 354 F.3d 1320, 1326 (11th Cir. 2003) ("A federal district court has personal jurisdiction to try any defendant brought before it on a federal indictment charging a violation of federal law.") (citing United States v. Alvarez-Machain, 504 U.S. 655, 659–70 (1992)); *see also infra* notes 265–267.

242. *In re* Sealed Case, 932 F.3d 915, 922–27 (D.C. Cir. 2019); *In re* Sealed Case, 832 F.2d 1268, 1272–74 (D.C. Cir. 1987), *abrogated by* Braswell v. United States, 487 U.S. 99 (1988); *In re* Marc Rich & Co., 707 F.2d 663, 666–70 (2d Cir. 1983). For analysis of the personal jurisdiction distinction between criminal defendants and third parties from which disclosure is compelled during criminal investigations, see United States v. Halkbank, No. 15 CR. 867 (RMB), 2020 WL 5849512, at *7 (S.D.N.Y. Oct. 1, 2020); United States v. Turkiye Halk Bankasi A.S., 426 F. Supp. 3d 23, 37–38 (S.D.N.Y. 2019); and United States v. Maruyasu Indus. Co., 229 F.Supp.3d 659, 669 (S.D. Ohio 2017).

IV. CAN THE UNITED STATES MAKE FULL USE OF CLOUD ACT AGREEMENTS?

The two potential benefits CLOUD Act agreements provide at international law should now be clear. While commentary to date doubts the United States' motivation to use these agreements at all[243]—a view Part III critiqued—the United States' legal ability to take advantage of the first benefit, minimizing conflicts, as a matter of domestic U.S. law does not appear to be questioned.[244] In contrast, the United States has expressly denied that CLOUD Act agreements give it any greater scope to gain data from foreign service providers.[245] Part IV primarily critiques that view, as well as the related argument that this analysis is merely theoretical.

A. Personal Jurisdiction Under The Due Process Clause And CLOUD Act Agreements

(1) The U.S.-UK Agreement Enhances U.S. Law Enforcement's Ability To Assert "Minimum Contacts" Over Foreign Service Providers

Even if we assume, as the *White Paper* does, that a U.S. court must be satisfied that the "minimum contacts" test for personal jurisdiction is fulfilled before an SCA order to a foreign service provider will be made,[246] the U.S.-UK Agreement may contribute to a finding that minimum contacts exist—if not supply sufficient contacts altogether. Where a federal court is asked to issue an SCA order, the Fifth Amendment, which protects both legal and natural persons,[247] governs the personal jurisdiction Due Process

243. *See supra* text accompanying notes 66–75.

244. *See supra* note 97. The CLOUD Act does, curiously, include a new enhanced comity defense, sitting alongside the existing common law test, *see supra* note 115, explained further at Part IV.B(2) below. CLOUD Act, § 103(b), 18 U.S.C. § 2703(h). The existence of this new defense may imply a failure to appreciate the private international law benefit of CLOUD Act agreements by drafters, as it appears largely redundant. Since CLOUD Act agreements require each state to lift all blocking statutes in their own law, *see supra* Part II.A(1), providers would only face a material risk of violating the law of a CLOUD Act agreement member state if that state had failed to implement this obligation or if, despite the ease, U.S. law enforcement failed to channel an SCA request through a CLOUD Act agreement. *See supra* text accompanying note 117.

245. *See supra* notes 76–84.

246. *See supra* notes 81–76.

247. N. Sec. Co. v. United States, 193 U.S. 197, 24 S. Ct. 436, 444 (1904); *see* Johnathon W. Ellison, *Trust the Process? Rethinking Due Process and the President's Emergency Powers over the Digital Economy*, 71 DUKE L.J. 499, 531 (2021) (discussing "technology companies" in particular).

inquiry.[248] As the SCA permits nationwide service,[249] the "forum" with which the recipient of the order must have minimum contacts is the United States overall.[250] The Supreme Court has indeed repeatedly emphasized that "it is the defendant's conduct that must form the necessary connection with the forum State that is the basis for its jurisdiction over him."[251] Following enactment of the CLOUD Act, many foreign service providers now

248. Dusenbery v. United States, 534 U.S. 161, 167 (2002) (The Due Process Clause of the Fifth Amendment prohibits the United States, as the Due Process Clause of the Fourteenth Amendment prohibits the States, from depriving any person of property without 'due process of law.'); Malloy v. Hogan, 378 U.S. 1, 26 (1964) ("Due process of law is secured against invasion by the federal Government by the Fifth Amendment, and is safeguarded against state action in identical words by the Fourteenth.") (quoting Betts v. Brady, 316 U.S. 455, 462 (1942)); *e.g.*, United States v. Leora, 333 F. Supp. 3d 172, 184 (E.D.N.Y. 2018) (evaluating whether extraterritorial digital searches "violate[d] defendant's Fifth Amendment due process rights"); *see also In re* Search Warrant Issued to Google, Inc., 264 F. Supp. 3d 1268, 1272 (N.D. Ala. 2017) (implying that Due Process personal jurisdiction analysis for the purposes of the SCA is undertaken "pursuant to the Fifth Amendment's Due Process Clause") (quoting Republic of Panama v. BCCI Holdings (Luxembourg) S.A., 119 F.3d 935, 942 (11th Cir. 1997)). *See generally* United States v. Lanza, 260 U.S. 377, 382 (1922) ("The Fifth Amendment, like all the other guaranties in the first eight amendments, applies only to proceedings by the federal government."). For discussion of jurisdictional issues arising when a state court issues an SCA order, see Peters et al., *supra* note 7, at 1079–84.

249. United States v. Ackies, 918 F.3d 190, 201–02 (1st Cir. 2019); United States v. Bansal, 663 F.3d 634, 662 (3d Cir. 2011); United States v. Berkos, 543 F.3d 392, 396–98 (7th Cir. 2008); *see* United States v. Scully, 108 F. Supp. 3d 59, 75–83 (E.D.N.Y. 2015) (outlining the history of the SCA's nationwide service provision and collecting cases on this point).

250. "Unless a federal statute otherwise provides," a federal court's jurisdiction "is keyed to that of a court of general jurisdiction in the state in which it sits," in which case "the scope of the minimum-contacts inquiry" by the federal court mirrors what it "would be under the Fourteenth Amendment for a claim in state court: confined to contacts with the forum state." *In re* Sealed Case, 932 F.3d 915, 924–25 (D.C. Cir. 2019). Where a federal statute provides for nationwide service, however, courts have held that the "the Fifth Amendment requires only 'minimum contacts with the United States' as a whole—rather than with the forum state." *Id.* (citing SEC v. Bilzerian, 378 F.3d 1100, 1106 n.8 (D.C. Cir. 2004)); Livnat v. Palestinian Auth., 851 F.3d 45, 55 (D.C. Cir. 2017); *see* Stephen E. Sachs, *The Unlimited Jurisdiction of the Federal Courts*, 106 VIRG. L. REV. 1703, 1704 n.6 (2020) (collecting authorities). *But see* Bristol-Myers Squibb Co. v. Superior Ct. of Cal., 137 S. Ct 1773, 1783–84 (2017) (leaving this point open); *see also Livnat*, 851 F.3d at 55 n.6 ("Some courts have also suggested that under the Fifth Amendment, even if the defendant has sufficient nationwide contacts, a plaintiff must additionally justify jurisdiction in the particular state.").

251. Walden v. Fiore, 571 U.S. 277, 284 (2014); *see id.* ("We have consistently rejected attempts to satisfy the defendant-focused 'minimum contacts' inquiry by demonstrating contacts between the plaintiff (or third parties) and the forum State."); Ford Motor Co. v. Mont. Eighth Jud. Dist. Ct., 141 S. Ct. 1017, 1025 (2021) ("The plaintiff's claims, we have often stated, 'must arise out of or relate to the defendant's contacts' with the forum."); Burger King Corp. v. Rudzewicz, 471 U.S. 462, 475 (1985) ("The relationship must arise out of contacts that the defendant himself creates with the forum State."); *c.f.*, Asahi Metal Indus. Co. v. Super. Ct. of Cal., 480 U.S. 102, 112 (1987) ("The placement of a product into the stream of commerce, without more, is not an act of the defendant purposefully directed toward the forum State."). The Supreme Court has also recently suggested a strict approach to assessing a corporation's contacts with the United States is appropriate, albeit in a very different context. *E.g.*, Nestle USA, Inc. v. Doe, 141 S. Ct. 1931, 1937 (2021) (considering when corporate actions "establish domestic application of the" Alien Tort Statute, 28 U.S.C. § 1350).

expressly market themselves as being beyond U.S. jurisdiction.[252] At face value, it is therefore initially attractive to suppose a U.S. court would reject an SCA application directed to such foreign service providers, assuming the providers had not, at least, deliberately sought out U.S. clients or made equivalent contacts with the United States.[253] But whether this remains true for UK service providers is far from clear following the U.S.-UK Agreement.

In *Ford Motor Co. v. Montana Eighth Jud. Dist. Ct.,* the Supreme Court restated the purpose of its personal jurisdiction requirements, saying these "derive from and reflect two sets of values—treating defendants fairly and protecting 'interstate federalism.'"[254] Fairness requires that parties have notice or "fair warning—knowledge that a particular activity may subject [them] to the jurisdiction of a foreign sovereign."[255] A U.S. court may ultimately consider that the U.S.-UK Agreement provides or supports such notice to UK service providers. Nearly two years have now elapsed since this international agreement was announced by the two countries as providing the United States with "reciprocal access" to data from UK service providers.[256] Its reciprocal nature was emphasized repeatedly during UK Parliamentary debates and related materials,[257] as well as in other UK commentary.[258] A court may conclude that service providers subject to UK

252. *See supra* note 223 and accompanying text.

253. *See* U.S. WHITE PAPER, *supra* note 9, at 8 ("The more a company has purposefully directed its conduct into the United States, the more likely a court will find the company is subject to U.S. jurisdiction.").

254. *Ford Motor Co.*, 141 S. Ct. at 1025 (quoting World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 293 (1980)).

255. *Id.* (quoting *Burger King*, 471 U.S. at 472); *see* Quill Corp. v. North Dakota, 504 U.S. 298, 312 (1992) ("We have . . . often identified "notice" or "fair warning" as the analytic touchstone of due process nexus analysis."), *overruled on other grounds by* South Dakota v. Wayfair, Inc., 138 S. Ct. 2080 (2018).

256. *See supra* note 71.

257. *E.g.*, HL Deb (11 July 2018) (792) col. 924 (remarks of Lord Rosser) ("[T]he CLOUD Act . . . requires that when the [U.S.]concludes an agreement with another country, such as the UK, that country must allow the [U.S.] reciprocal rights of data access."); HL Deb (5 Sept. 2018) (792) col. 136GC (remarks of Lord Paddick) ("[P]resumably the countries that enter into international co-operation agreements with the UK . . . will expect their own law enforcement agencies to be able to apply through their own domestic courts for equivalent orders that would allow them to seek stored electronic data directly from service providers based in the UK; the reciprocal agreement."); Crime (Overseas Production Orders) Bill 2018-19, HL Bill [293] Explanatory Notes ¶ 18 (UK) ("Any international agreement between the UK and another country may be reciprocal, allowing law enforcement agencies in that country to require that data is produced by companies based in the UK.").

258. *E.g.,* Barnett, Black & Manson, *supra* note 89 ("The [U.S.-UK] Agreement creates a reciprocal framework which also allows for the transfer of data from the UK to the U.S."); Shaul Brazil & Jonathan Flynn, *Overseas Production Orders – A New Tool for UK Law Enforcement*, BCL SOLICITORS LLP (Feb. 26, 2019), https:// www.bcl.com/ overseas- production- orders-a- new-tool-for- uk-law-enforcement/ ("[CLOUD Act regime agreements] enable 'qualifying foreign governments' to request electronic data from the [U.S.] in exchange for reciprocal arrangements that allow the [U.S.] to request electronic data from that country.").

(and now, potentially U.S.) jurisdiction have had sufficient notice and thus ample time to re-structure their affairs off-shore to avoid exposure if necessary.[259] That approach is supported by analogous criminal precedents.[260] Of course, the civil and criminal personal jurisdiction requirements typically differ markedly.[261] Nonetheless, U.S. courts may draw on criminal precedents, given the underlying criminal context of the U.S.-UK Agreement and SCA.[262] As noted, the U.S.-UK Agreement provides the United Kingdom's international law consent to the United States expanding jurisdiction over UK service providers.[263] U.S. courts often hold that foreign state consent, whether provided thorough an international agreement or merely informally,[264] provides personal jurisdiction over foreign defendants seized overseas.[265] For example, the majority of U.S. Circuits to have determined the jurisdictional reach of the Maritime Drug Law Enforcement Act (MDLEA), which provides for extraterritorial

259. *See Ford Motor Co.*, 141 S. Ct. at 1025 (noting that, given "fair warning," "[a] defendant can thus 'structure [its] primary conduct' to lessen or avoid exposure to a given [country's] courts.") (quoting *World-Wide Volkswagen*, 444 U.S. at 297).

260. *See also* Dan E. Stigall, *International Law and Limitations on the Exercise of Extraterritorial Jurisdiction in U.S. Domestic Law*, 35 HASTINGS INT'L & COMP. L. REV. 323, 377–80 (2012) (discussing the limits of such an approach but recognizing that areas of law may be on a continuum between civil and criminal).

261. *See supra* notes 240–241 and accompanying text..

262. Both are intended to further criminal investigations. The U.S.-UK Agreement allows orders "for the purpose of obtaining information relating to the prevention, detection, investigation, or prosecution" of certain serious crimes. *See* U.S.-UK Agreement, *supra* note 2, arts. 1(5), 1(11), 4(1), 10(3). SCA orders must be sought to obtain "evidence of a crime," to otherwise obtain data "relevant and material to an ongoing criminal investigation," or similar. 18 U.S.C. § 2703(a), (d) (partly incorporating FED. R. CRIM. P. 41(c)).

263. *See supra* note 173 and accompanying text.

264. *See* United States v. Robinson, 843 F.2d 1, 4 (1st Cir. 1998); *see also supra* note 172 (setting out the same position at international law that foreign state consent may be provided informally).

265. *E.g.*, United States v. Brehm, 691 F.3d 547, 553 (4th Cir. 2012) ("With Afghanistan having disclaimed any interest in prosecuting criminal conduct [pursuant to an international agreement with the United States] by those situated similarly to Brehm, due process is not offended by the United States stepping into the jurisdictional void."); United States v. Cardales, 168 F.3d 548, 553 (1st Cir. 1999) ("[A] state has jurisdiction to prescribe and enforce a rule of law in the territory of another state to the extent provided by international agreement with the other state."); United States v. Martinelli, 62 M.J. 52, 81 (C.A.A.F. 2005) ("Appellant's prosecution for these crimes [overseas] was not merely tolerated by German authorities, it was officially condoned pursuant to an international treaty."); *see* Laker Airways Ltd. v. Sabena, Belgian World Airlines, 731 F.2d 909, 932 (D.C. Cir. 1984) (noting, in a civil context, that "far from conferring any immunity [as defendants claimed], *their treaties contain express language subjecting them to the jurisdiction of the United States over predatory pricing and abuse of monopoly power*."); *see also* United States v. Al Kassar, 660 F.3d 108, 119 (2d Cir. 2011) ("Fair warning does not require that the defendants understand that they could be subject to criminal prosecution *in the United States* so long as they would reasonably understand that their conduct was criminal and would subject them to prosecution somewhere."). *See generally* Bruce A. Baird, *Stranger in a Strange Land: Asserting Criminal Jurisdiction Over Strangers*, 8 VA. J. CRIM. L. 1 (2020) (elaborating on criminal jurisdiction in the United States over noncitizen, nonresident defendants).

enforcement of drug laws at sea,[266] have held that consent by the flag state is sufficient for the United States to assert personal jurisdiction over ships at sea.[267]

In any event, "considerations sometimes serve to establish the reasonableness of jurisdiction upon a lesser showing of minimum contacts than would otherwise be required."[268] In the international context, the "interstate federalism" issues that the second stage of this analysis (i.e. reasonableness) would normally take into account transform:[269] before permitting personal jurisdiction over foreign persons, a court should "consider the procedural and substantive policies of other *nations* whose interests are affected by the assertion of jurisdiction," "as well as the Federal interest in" the United States' own "foreign relations policies."[270] Although these international factors often countenance against permitting extraterritorial personal jurisdiction, they predominantly point in the opposite direction here. Permitting extraterritorial personal jurisdiction over UK service providers by U.S. law enforcement will further, rather than undermine, both the United States' and United Kingdom's policy goals of preventing, detecting, investigating, and prosecuting crime.[271] This is after

266. Maritime Drug Law Enforcement Act, 46 U.S.C. § 705 *et seq.* (2018). While personal jurisdiction questions under MDLEA also engage the Fifth Amendment, MDLEA's extraterritorial reach has in part turned on particular Constitutional provisions relating to the sea. *See* United States v. Carvajal, 925 F. Supp. 2d 219, 249–60 (D.D.C. 2013). Nonetheless, its analysis of personal jurisdiction in the criminal arena coheres with examples in other criminal contexts. *See supra* note 265.

267. United States v. Baston, 818 F.3d 651, 669–70 (11th Cir. 2016); United States v. Perez-Oviedo, 281 F.3d 400, 402–03 (3d Cir. 2002); United States v. Bustos-Useche, 273 F.3d 622, 627–28 (5th Cir. 2001); United States v. Greer, 285 F.3d 158, 175–76 (2d Cir. 2000); *Cardales*, 168 F.3d at 553. The Ninth Circuits requires a "nexus" in this context—similar to "minimum contacts"—even where flag state consent arises. *E.g.*, United States v. Perlaza, 439 F.3d 1149, 1169 (9th Cir. 2006) ("[C]onsent . . . does not eliminate the nexus requirement").

268. Burger King Corp. v. Rudzewicz, 471 U.S. 462, 477 (1985); *see also* Gourdine v. Karl Storz Endoscopy-Am., Inc., 223 F. Supp. 3d 475, 483 (D.S.C. 2016) ("'[M]inimum contacts' and 'reasonableness' are not independent requirements; rather, they are aspects of the [overall] requirement[s] of due process.") (citing *Burger King*, 471 U.S. at 477); Henry H. Perritt, Jr., *Jurisdiction in Cyberspace*, 41 VILL. L. REV. 1, 15 n.53 (1996) ("The best way to combine the two considerations is to realize that when minimum contacts analysis results in a close question, fair play and substantial justice factors should have greater weight."). Various Circuits have offered similar views. *See* Yahoo! Inc. v. La Ligue Contre Le Racisme, 433 F.3d 1199, 1210 (9th Cir. 2006); OMI Holdings, Inc. v. Royal Ins. Co., 149 F.3d 1086, 1092 (10th Cir. 1998); Metro. Life Ins. Co. v. Robertson-Ceco Corp., 84 F.3d 560, 568 (2d Cir. 1996); Ticketmaster-New York, Inc. v. Alioto, 26 F.3d 201, 210 (1st Cir. 1994).

269. *See supra* note 254.

270. Asahi Metal Indus. Co. v. Super. Ct. of Cal., 480 U.S. 102, 115 (1987); *see also id.* at 115 (emphasizing that a "careful inquiry . . . into reasonableness" is required in the international context); Daimler AG v. Bauman, 571 U.S. 117, 140 (2014) (similarly recognizing that "the transnational context of this dispute bears attention"); Int'l Techs. Consultants, Inc. v. Euroglas S.A., 107 F.3d 386, 394 (6th Cir. 1997) (noting that the interests of "foreign nation[s] . . . merit particular respect in [U.S.] courts").

271. *See* Data Access Agreement Press Release, *supra* note 3 (quoting representatives of both

all the precise aim of the U.S.-UK Agreement, a primary function of which is to permit expanded personal jurisdiction by removing blocking statutes.[272] Such U.S. extraterritorial personal jurisdiction, moreover, will merely mirror and thus be reciprocal with the United Kingdom's own plans.[273] Against this, potentially, are the interests of other states who may claim jurisdiction over persons and/or data—similar to the UK "subject matter jurisdiction" analysis above.[274] Nearly all additional factors typical to assessing reasonableness are, however, supportive.[275] For example, the "judicial system's interest in obtaining the most efficient resolution of controversies" favors extraterritoriality;[276] the alternative—requiring U.S. law enforcement to obtain data from UK service providers through MLA or similar methods—would likely take months or years.[277] The only other factor pointing away, the "burden on the defendant," would likely be given little weight in this

countries emphasizing the significance of these policies); *e.g.*, In re Nazi Era Cases Against German Defendants Litig., 320 F. Supp. 2d 402, 231 (D.N.J. 2004), *aff'd*, 153 F. App'x. 819 (3d Cir. 2005) ("It would be hard to find a case where the procedural and substantive policies of another country would be more affected by the assertion of state jurisdiction than this case."); *see also* Kiobel v. Royal Dutch Petroleum Co., 569 U.S. 108, 124 (2013) ("[A]ccepting petitioners' view would imply that other nations, also applying the law of nations, could hale our citizens into their courts for alleged violations of the law of nations occurring in the United States, or anywhere else in the world."); *cf. Daimler*, 571 U.S. at 141–42 (warning that "expansive views" of personal jurisdiction over foreign persons may interfere with foreign states' actions, as well as the United States' "negotiation of international agreements").

272. *See supra* Part III.B; *see also, e.g.*, Oceanografia v. Hernandez, No. 13-10-00223-CV, 2011 WL 6142789, at *11–12 (Tex. App. Dec. 8, 2011) (similarly noting that the United States and Mexico "have a shared . . . interest" through an international agreement and concluding that there were "strong interests on both sides of the border in this case to enforce the trial court's personal jurisdiction") (citing McGee v. Int'l Life Ins. Co., 355 U.S. 220 (1957)). The interests the Agreement seeks to further would be viewed as substantial by U.S. courts. *See, e.g.*, Synthes (U.S.A.) v. G.M. Dos Reis Jr. Ind. Com. De Equip. Medico, 563 F.3d 1285, 1299 (Fed. Cir. 2009) (referring to the United States' "'substantial interest' in enforcing . . . laws" as relevant to the reasonableness of its assertion of personal jurisdiction over foreign parties); *see also* Reyes v. Marine Mgmt. & Consulting, Ltd., 586 So. 2d 103, 117 (La. 1991) ("Other nations likewise have an interest in seeing that their residents have redress for injuries and in seeing that actions against their corporations are tried in appropriate forums."). *See generally* Brabeau v. SMB Corp., 789 F. Supp. 873, 878 (E.D. Mich. 1992) ("Every state wishes to shield its citizens from harm and provide an avenue for redress.").

273. *See supra* Part III.B(1). *See generally Daimler*, 571 U.S. at 151 (cautioning that the United States should act with "reciprocal fairness" when asserting extraterritorial personal jurisdiction).

274. *See supra* text accompanying notes 184–204 (outlining the UK's subject matter jurisdiction jurisprudence); *e.g.*, Simon v. Philip Morris, Inc., 86 F. Supp. 2d 95, 135 (E.D.N.Y. 2000) ("England is not the only nation whose policies could be impinged upon by the exercise of personal jurisdiction [here]. The interests of the European Union are also affected.").

275. *See Asahi Metal Indus. Co.*, 480 U.S. at 115 (synthesizing these in the international context) (citing World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 292 (1980)). These factors include "the interests of the forum State, and the plaintiff's interest in obtaining relief." *Id.* at 113. Here, U.S. law enforcement is the titular plaintiff, while the "forum" is the United States itself. The United States has substantial interests in asserting extraterritorial personal jurisdiction here. *See supra* note 272.

276. *World-Wide Volkswagen Corp.*, 444 U.S. at 292.

277. *See supra* Part II.A.

context, where the "defendant" is a mere "disinterested third party" not at risk of "defending a full-scale trial proceeding."[278]

(2) "Minimum Contacts" And/Or Due Process Altogether May Be Entirely Inapplicable

The preceding section assumed the correctness of the *White Paper*'s claim that "minimum contacts" personal jurisdiction would be necessary to assert jurisdiction over foreign service providers under CLOUD Act agreements. This is, however, seriously arguable. It is questionable whether a minimum contacts analysis of the type attempted above is appropriate in this context or indeed under the Fifth Amendment altogether. The circumstances in which service providers may be within the personal jurisdiction of the United States given a mere "virtual" presence through Internet operations has been questioned but left undetermined by the Supreme Court.[279] The Court also very recently indicated it may abandon the entire "minimum contacts" framework of *International Shoe* entirely in *Ford Motor Co*.[280] Lower courts have also referred to "[t]he case law discussing the specific issue of personal jurisdiction over foreign corporations in the criminal context"—arguably relevant here[281]—as "surprisingly sparse and poorly developed."[282] Any of these ambiguities may be seized upon to support extraterritorial personal jurisdiction over foreign service providers in this context.

---

278. U.S. DEP'T OF JUSTICE, *supra* note 7, at 112; SEC v. Marin, 982 F.3d 1341, 1351 (11th Cir. 2020); *see* In re Search Warrant, No. 6:05-MC-168-ORL-31JGG, 2005 WL 3844032, at *5 n.14 (M.D. Fla. Feb. 13, 2006) ("The only person conceivably being inconvenienced is the third party that owns the out-of-district property subject to the search warrant, but as a practical matter, such inconvenience is de minimis."); *see also* Theunissen v. Matthews, 935 F.2d 1454, 1462 (6th Cir. 1991) (suggesting the burden on a foreign defendant was relatively low because "the judicial systems of Canada and the United States are rooted in the same common law traditions," a comparison that could also be made about the United Kingdom).

279. *See* Ford Motor Co. v. Mont. Eighth Jud. Dist. Ct., 141 S. Ct. 1017, 1028–29 n.4 (2021) ("[W]e do not here consider internet transactions, which may raise doctrinal questions of their own."); Walden v. Fiore, 571 U.S. 277, 290 n.9 (2014) ("[T]his case does not present the very different questions whether and how a defendant's virtual 'presence' and conduct translate into 'contacts' with a particular State.").

280. Justice Gorsuch, supported by Justice Thomas, criticized "*International Shoe*'s increasingly doubtful dichotomy." *See Ford Motor Co.*, 141 S. Ct. at 1036–39 (Gorsuch, J., concurring). Justice Alito expressed similar concerns, questioning "whether the case law we have developed . . . is well suited for the way in which business is now conducted." *Id.* at 1032 (Alito, J., concurring). The majority opinion referred to Justice Alito's concurrence as "[f]air enough perhaps." *Id.* at 1025 n.2. *International Shoe*'s days may be numbered.

281. *See supra* note 262 and accompanying text..

282. United States v. Chitron Elecs. Co., 668 F. Supp. 2d 298, 302–04 (D. Mass. 2009); *see* In re Sealed Case, 932 F.3d at 922 (quoting Boyd v. Meachum, 77 F.3d 60, 66 (2d Cir. 1996)) ("While the federal constitutional requirements of personal jurisdiction in a civil setting are reasonably well-defined . . . this is not so in a criminal case.").

While each of these ambiguities applies equally to the Fourteenth Amendment's Due Process Clause, consideration of the Fifth Amendment's Due Process Clause invites even greater uncertainty. The Supreme Court has expressly left open "whether the Fifth Amendment imposes the same restrictions on the exercise of personal jurisdiction by a federal court" as required by a state court under the Fourteenth Amendment.[283] Although the various circuits have historically assumed the Fifth Amendment requires a similar analysis,[284] this is changing: in an opinion now vacated pending rehearing *en banc*, the Fifth Circuit suggested that there are "meaningful differences" between the Fifth and Fourteenth Amendments in this context,[285] emphasizing the uncertainties of existing Fifth Amendment jurisprudence.[286] Similar views have been debated in the literature for decades.[287] Professor Stephen E. Sachs recently argued that the United States "may well have authority to extend federal personal jurisdiction" internationally "beyond the scope of 'minimum contacts' doctrine."[288] In comments that appear directly applicable here, Sachs suggested that "if a foreign nation authorized the United States to exercise jurisdiction within its borders . . . Congress might be able to take them up on the offer," including by exercising jurisdiction over "contactless foreigners."[289]

283. Bristol-Myers Squibb Co. v. Superior Ct. of Cal., 137 U.S. 1773, 1784 (2017); *see* Sachs, *supra* note 250, at 1704–05 ("Without Supreme Court precedent on point, the courts of appeals all agree that the Fifth Amendment requires at least the sorts of national contacts that the Fourteenth Amendment requires of a state."). *See generally* Douglass v. Nippon Yusen Kabushiki Kaisha, 996 F.3d 289, 294 (5th Cir. 2021), *reh'g en banc granted, vacated sub nom.* Douglass v. Kaisha, 2 F.4th 525 (5th Cir. 2021) ("The Supreme Court has opined and elaborated on the Fourteenth Amendment's due process requirements and not on the Fifth's.").

284. *See supra* note 250.

285. *Douglass*, 996 F.3d at 295–96.

286. *See id.* at 296 ("Only one of our sister circuits has thoroughly analyzed whether, in this context, the Fourteenth Amendment and Fifth Amendment standards are the same . . . . We find unpersuasive [its] conclusion that Fifth Amendment due process standards must track those imposed by the Fourteenth Amendment.") (citing Livnat v. Palestinian Auth., 851 F.3d 45, 55 (D.C. Cir. 2017)).

287. *Compare* Lea Brilmayer & Charles Norchi, *Federal Extraterritoriality and Fifth Amendment Due Process*, 105 HARV. L. REV. 1217, 1262–63 (1992) (arguing that the Fifth Amendment should impose substantial limits on the United States' ability to enact extraterritorial legislation), *with* A. Mark Weisburd, *Due Process Limits on Federal Extraterritorial Legislation?*, 35 COL. J. TRANS. L. 379, 427 (1997) (disagreeing and concluding that the Fifth Amendment imposes no territorial limitations on the "extent to which Congress can enact legislation with extraterritorial effect"); *see also, e.g.*, Anthony J. Colangelo, *A Unified Approach to Extraterritoriality*, 97 VA. L. REV. 1019, 1107 (2011) ("[I]t is far from clear that Fifth Amendment due process even cares about other nations' sovereignty interests."). These chime with similar concerns in related regulatory fields. *See* Buxbaum, supra *note* 174, at 280–93.

288. Sachs, *supra* note 250, at 1728; *see id.* at 1729 ("In general, Congress can extend the federal courts' personal jurisdiction as far as it wants.").

289. *Id.* at 1729–31.

This debate has been fermented in part by the increasingly nationalistic approach to constitutional rights in U.S. courts—potentially providing a further reason for doubting that the Fifth Amendment's Due Process clause constrains extraterritorial U.S. law enforcement action here. The Supreme Court has recently stated that "it is long settled as a matter of American constitutional law that foreign citizens outside U. S. territory do not possess rights under the U. S. Constitution."[290] Such rights apparently only crystalize when foreign persons have traveled to the United States and developed substantial connections there.[291] Regardless of the correctness of that position,[292] it echoes—and significantly expands—the curtailing of foreign persons' constitutional rights undertaken by the Court in recent decades.[293] As scholars and courts have recognized, this curtailment of rights raises an obvious "paradox" for a personal jurisdiction analysis in the context of a foreign person: the precise factor that should ordinarily allow foreign parties to dispute personal jurisdiction—a lack of "minimum contacts" with the

290. Agency for Int'l Dev. v. All. for Open Soc'y Int'l, Inc., 140 S. Ct. 2082, 2086 (2020).

291. United States v. Verdugo-Urquidez, 494 U.S. 259, 265–75 (1990).

292. *See, e.g.*, *Agency for Int'l Dev.*, 140 S. Ct. at 2099–2100 (Breyer, J., dissenting) (doubting this analysis, stating that "the majority's blanket assertion about the extraterritorial reach of our Constitution does not reflect the current state of the law"). I have critiqued this in relation to CLOUD Act agreements and the Fourth Amendment elsewhere. *See* Cochrane, *supra* note 33, at 90–97.

293. Zadvydas v. Davis, 533 U.S. 678, 693 (2001); *Verdugo-Urquidez*, 494 U.S. at 265–75; Johnson v. Eisentrager, 339 U.S. 763, 785 (1985). This approach also predominates within the D.C. Circuit in particular. *See, e.g.*, Bade v, De't if State, No. 21-CV-01678 (APM), 2021 WL 3403938, at *2 (DD.C. Aug. 4, 2021); Deripaska v. Yellen, No. 19-CV-00727(APM), 2021 WL 2417425, at *11 (D.D.C. June 13, 2021), *appeal filed* (D.C. Cir. July 8, 2021) (concluding that defendant "lacks standing to pursue his due process challenge to his designations"); Al Hela v. Trump, 972 F.3d 120, 138–50 (D.C. Cir. 2020) ("[A]s an alien detained outside the sovereign territory of the United States, [appellant] may not invoke the protection of the Due Process Clause."); Ali v. Trump, 959 F.3d 364, 379 (D.C. Cir. 2020) (Randolph, S.C.J., concurring) ("The detainees were not entitled to the protection of the Due Process Clause because the Supreme Court has decided that aliens outside of the United States do not qualify as 'any person' within the meaning of the Fifth Amendment.").

United States—is the same factor that apparently stops them from raising this objection.[294] There is no consensus on how to resolve this.[295]

Personal jurisdiction law in the United States in "doctrinal disarray."[296] The purposes of the analysis above is not to predict, and certainly not to guide, U.S. law enforcement or courts as to the proper approach to personal jurisdiction in this context. Instead, it seeks to underscore the uncertainty here. Ultimately, were U.S. law enforcement to attempt to assert personal jurisdiction over UK service providers, even ones entirely lacking "minimum contacts" with the United States, there is therefore a real possibility this would be sanctioned by a U.S. court—even putting the U.S.-UK Agreement to one side. While these findings would be significant, even if the prospect of such expanded jurisdiction were merely theoretical, the final section of Part IV explains that such expanded jurisdiction may already be entirely possible.

B. The Prospect of U.S. Law Enforcement Expanding Jurisdiction Over Foreign Service Providers Is Not Merely Theoretical

(1) The United States Is Not Bound By The White Paper

This first point can be stated very briefly. The United States is not constrained by the narrow approach to personal jurisdiction it has taken in the *White Paper*. It is "purely informational."[297] To the extent it still

---

294. *E.g.*, Sachs, *supra* note 250, at 1741–42 (referring to this as "a doctrinal puzzle"); Austen L. Parrish, *Sovereignty, Not Due Process: Personal Jurisdiction Over Nonresident Alien Defendants*, 41 WAKE FOREST L. REV. 1, 33 (2006) ("Aliens abroad with no connection to the United States have no constitutional rights but, under current personal jurisdictional law, paradoxically have the strongest claim that the Due Process Clause prohibits a U.S. court from asserting jurisdiction over them."); GSS Grp. Ltd. v. Nat'l Port Auth., 680 F.3d 805, 815–16 (D.C. Cir. 2012) (referring to the debate over whether aliens who otherwise lack constitutional rights have due process rights for jurisdictional purposes); United States v. Ologeanu, No. 5:18-CR-81-REW-MAS, 2020 WL 1676802, at *27 n.34 (E.D. Ky. Apr. 4, 2020); *see also* FBME Bank Ltd. v. Lew, 209 F. Supp. 3d 299, 328 (D.D.C. 2016) (suggesting that a foreign corporation "ha[d] likely not met its burden to establish an entitlement to due process as a general matter") (citing *Verdugo-Urquidez*, 494 U.S. at 271). *See generally* Robin J. Effron, *Solving the Nonresident Alien Due Process Paradox in Personal Jurisdiction*, 116 MICH. L. REV. ONLINE 123, 129 (2018) (elaborating on these ideas).

295. *Compare, e.g.*, Douglass v. Nippon Yusen Kabushiki Kaisha, 996 F.3d 289, 295 (5th Cir.), *reh'g en banc granted, vacated sub nom.* Douglass v. Kaisha, 2 F.4th 525 (5th Cir. 2021) ("[F]airness concerns suggest that the Fifth Amendment's clause should preclude foreign nonresident defendants with no ties to the United States from being called upon to defend suits in the United States."), *with* Sachs*, supra* note 250, at 1743 ("If Congress wants to summon the coffee farmers and shirtmakers of the world, it can.").

296. Anthony J. Colangelo, *What is Extraterritorial Jurisdiction?*, 99 CORNELL L. REV. 1303, 1324 (2014).

297. Ben Barnett et al., *Actual Impact of 2018 U.S. CLOUD Act Still Hazy*, DECHERT (July 22, 2019), https://info.dechert.com/10/12598/july-2019/actual-impact-of-2018-u.s.-cloud-act-still-hazy.asp?sid= 0a 0 05 ac3-1df4-43c4-a944- f723188079ce# ("[S]uch white papers – should they be viewed as 'guidance

represents the United States' good faith interpretation of the U.S.-UK Agreement,[298] there is no impediment on the United States changing this interpretation swiftly.[299] Ultimately, it will be for U.S. courts to interpret the U.S.-UK Agreement.[300]

In any event, while the *White Paper* leaves its reader with the impression that nothing much has changed,[301] when read closely it actually appears to leave scope for CLOUD Act agreements to be used to expand personal jurisdiction in the manner articulated above. Even assuming a "minimum contacts" personal jurisdiction analysis is applicable—a debatable point[302]—while a CLOUD Act agreement will not "by itself" expand U.S. law enforcement's personal jurisdiction over foreign service providers,[303] it may at least facilitate such an expansion of jurisdiction, as part of a "fact-specific inquiry" into personal jurisdiction.[304]

---

documents' – are purely informational, do not rise to the level of regulation or rule, and are not legally binding on the Department.") (citing U.S. Dep't of Just., Just. Manual §1-19.000 (2018)); *cf.* Perez v. Mortg. Bankers Ass'n, 575 U.S. 92, 95–97 (2015) (elaborating on the circumstances in which federal agencies must consult before changing their own interpretations of rules).

298. This is arguably doubtful because the U.S.-UK Agreement post-dates the White Paper. *Compare* U.S.-UK AGREEMENT, *supra* note 2, at 10 (dated Oct. 2019), *with* U.S. WHITE PAPER, *supra* note 9, at 1 (dated Apr. 2019).

299. *E.g.*, *Statement by NSC Spokesperson Bernadette Meehan on the U.S. Presentation to the Committee Against Torture*, WHITE HOUSE (Nov. 12, 2014), https:// obamawhitehouse. archives.gov/the-press- office/ 2014/11/12/statement-nsc-spokesperson-bernadette-meehan-us-presentation-committee-a (announcing changes to the U.S. government's interpretation of an international agreement). *But see* Rahim Moloo, *Changing Times, Changing Obligations? The Interpretation of Treaties Over Time*, 106 AM. SOC'Y INT'L L. PROC. 261, 263 (2012) ("If the parties engage in consistent conduct over a long period of time, thereby demonstrating agreement as to the interpretation of the treaty, that definition may become entrenched and may make it difficult to demonstrate that an evolved interpretation is permissible.").

300. RESTATEMENT (FOURTH) OF FOREIGN RELS. L. OF THE U.S. § 306 (AM. L. INST. 2018); *see also, e.g.*, Weinberger v. Rossi, 456 U.S. 25, 32–36 (1982) (treating an executive agreement as equivalent to a treaty for the purposes of statutory interpretation). While courts normally give "great weight" to the interpretation of the U.S. executive of an international agreement, *id.* § 152, that principle may have less force here, where the United States' interpretation appears to conflict with that given by its other treaty partner. *See also supra* note 227; *cf.* Sumitomo Shoji Am., Inc. v. Avagliano, 457 U.S. 176, 185 (1982) ("When the parties to a treaty both agree as to the meaning of a treaty provision, and that interpretation follows from the clear treaty language, we must, absent extraordinarily strong contrary evidence, defer to that interpretation.").

301. *See* U.S. WHITE PAPER, *supra* note 9, at 5, 14.

302. *See supra* Part IV.A(2).

303. *See* U.S. WHITE PAPER, supra note 9, at 4–5; UK EXPLANATORY MEMORANDUM, *supra* note 27, ¶ 7.

304. U.S. WHITE PAPER, supra note 9, at 8.

(2) Expanded Jurisdiction May Be Possible Without Any New Statutory Authority

Once the U.S.-UK Agreement comes into force, U.S. law enforcement may be able to make use of its public international law benefit—expanding jurisdiction to issue SCA requests to foreign service providers previously beyond its scope[305]—without any new statutory authority.[306] U.S. law also applies a "presumption against extraterritoriality."[307] It is commonly believed that, although the U.S. Congress has the authority to enact extraterritorial legislation,[308] it has declined to do so with the SCA and, as a result, its scope extends only to service providers operating within U.S. territory: indeed, the United States itself took this position during the *Microsoft Ireland* litigation.[309] In a largely overlooked comment during that dispute, however, Judge Raggi—dissenting from the Second Circuit's denial of rehearing *en banc*—suggested that whether the SCA could be used to compel disclosure from "foreign service providers" (otherwise) within U.S. personal jurisdiction was an open question.[310] In any event, the territoriality of the SCA should be revisited following enactment of the CLOUD Act and its SCA amendments.[311] The CLOUD Act's reciprocity requirement for agreements made under it requires foreign states to remove restrictions on "service providers, *including* providers subject to United States jurisdiction."[312] Here, "including" appears redundant if this amendment were intended to be limited to providers independently subject to U.S. jurisdiction.[313] The CLOUD Act also introduced a new enhanced comity test

305. *See infra* Part III.B.

306. *Contra supra* notes 76–83 (noting the U.S. position that its jurisdiction over service providers have not changed under the CLOUD Act or agreements made under it).

307. *See supra* note 188. *See generally* Morrison v. Nat'l Australia Bank Ltd., 561 U.S. 247, 255 (2010) (noting that federal laws are presumed to have only domestic application).

308. RESTATEMENT (FOURTH) OF FOREIGN RELS. L. OF THE U.S. § 404 (AM. L. INST. 2018).

309. The United States conceded the territoriality of the SCA in *Microsoft Ireland*. Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197, 210–20, 210 n.19 (2d Cir. 2016), *vacated and remanded sub nom.* United States v. Microsoft Corp., 138 S. Ct. 1186 (2018). Multiple other district courts have agreed with this interpretation. *See* In re Search of Info. Associated with Accounts Identified as [redacted]@gmail.com, 268 F. Supp. 3d 1060, 1068 (C.D. Cal. 2017) ("[A]ll the decisions [subsequent to *Microsoft Ireland*] agree, and the Government concedes, that the SCA is not extraterritorial.").

310. Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp, 855 F.3d 53, 74 (2d Cir. 2017) (Raggi J., dissenting) ("When such a case comes before us, we can certainly consider whether a court with personal jurisdiction over the foreign service provider can issue a § 2703(a) warrant compelling it to disclose in the United States communications stored abroad.").

311. *See supra* text accompanying notes 33–43.

312. CLOUD Act § 105(b), 18 U.S.C. 2523(b)(4)(i) (2018) (emphasis added).

313. *See generally* Bailey v. United States, 516 U.S. 137, 146 (1995) (applying an assumption that when Congress uses terms "it intend[s] each term to have a particular, nonsuperfluous meaning"). This new statutory language could, instead, have simply read "service providers subject to United States

into the SCA that expressly extends to "foreign communications service providers," enabling objections from them in certain circumstances where an SCA request would breach the laws of another CLOUD Act regime member state.[314] This language appears to make sense only if SCA requests may now reach foreign service providers.[315] The SCA may therefore already have extraterritorial force.

There may be alternative bases on which U.S. law enforcement could issue U.S.-UK Agreement requests to UK service providers. For example, although U.S. courts have overwhelmingly held—prior to the above amendments—that the SCA (and Wiretap Act) lack extraterritorial force,[316] "extraterritoriality" has a distinct and narrow meaning under U.S. law.[317] Most courts consider an SCA request to be territorial so long as the provider discloses data within U.S. territory, regardless of where it was retrieved from.[318] They have also adopted a "listening post" theory, by which wiretaps will not be extraterritorial so long as the U.S. agent is listening within U.S. territory,[319] even if the intercept is otherwise entirely foreign.[320] If methods

jurisdiction" if Congress's intention were not to enable expanded jurisdiction.

314. CLOUD Act § 103(b),18 U.S.C. § 2703(h)(2) (2018) ("A provider of electronic communication service to the public or remote computing service*, including a foreign electronic communication service or remote computing service*, that is being required to disclose pursuant to legal process issued under this section the contents of a wire or electronic communication of a subscriber or customer, may file a motion to modify or quash the legal process . . . .") (emphasis added); *see also* 5 E-COMMERCE AND INTERNET LAW § 49.16, Westlaw (database updated Apr. 2020) (recognizing that this new comity mechanism extends to foreign service providers); *supra* note 244.

315. *See also, e.g.*, United States v. Lyons, 740 F.3d 702, 718 (1st Cir. 2014) (similarly concluding that legislation that "explicitly applies to transmission between the United States and a foreign country" was extraterritorial).

316. *E.g.*, *In re* Search of Info. Associated with Accts. Identified as [redacted]@gmail.com, 268 F. Supp. 3d 1060, 1068 (C.D. Cal. 2017) (concluding that the SCA lacks extraterritorial force); Huff v. Spaw, 794 F.3d 543, 547 (6th Cir. 2015) (holding that the Wiretap Act lacks extraterritorial force) (internal citations omitted).

317. *See* Jennifer Daskal, *supra* note 194, at 354–65 (2015) (elaborating on the U.S. law approach to extraterritoriality in relation to territorial warrant authority).

318. *In re* Search Warrant Issued to Google, Inc., 264 F. Supp. 3d. 1268, 1271–72 (N.D. Ala. 2017); *In re* Search Warrant to Google, Inc., No. 16-4116, 2017 WL 2985391, at *3–4 (D.N.J. July 10, 2017); *c.f. In re* Search a Certain E-Mail Account, 829 F.3d 197, 219–21 (2d. Cir. 2016), *vacated and remanded sub nom.* United States v. Microsoft Corp., 138 S. Ct. 1186 (2018).

319. United States v. Jackson, 849 F.3d 540, 551–52 (3d Cir. 2017); United States v. Rodriguez, 968 F.2d 130, 136 (2d Cir. 1992); *see* Dahda v. United States, 138 S. Ct. 1491, 1495, 1499 (2018) (assuming, without deciding the correctness of this jurisprudence, that a wiretap falls within a District Court's territorial jurisdiction so long as the "listening post" is within that jurisdiction).

320. United States v. Rodriguez-Serna, No. 18cr3739 WQH, 2019 WL 4214389 (S.D. Cal. Sept. 5, 2019); United States v. Cano-Flores, 796 F.3d 83, 86 (D.C. Cir. 2015); United States v. Cosme, No. 10CR3044 WQH, 2011 WL 3740337 (S.D. Cal. 2011); Daskal, *Correcting the Record*, *supra* note 90. *Contra* United States v. Caro, No. CR 12-964-DMG, 2015 WL 13358234, at *2 (C.D. Cal. Dec. 2, 2015) ("[I]n order for the Government to intercept a call at a listening post located within the United States, the call would have to access a cellular tower on the United States network.").

were established to enable UK service providers to disclose or route data through U.S. territory in response to SCA or Wiretap Act orders, these orders may therefore be within the scope of these statutes.[321] This method does, however, likely rely on the willing cooperation of these providers. Alternatively, the territorial nature of these statutes may theoretically offer U.S. law enforcement greater freedom here. Responding to a claim that extraterritorial U.S. law enforcement surveillance breached the Wiretap Act, the D.C. Circuit stated that this "reflects a fundamental misunderstanding of the role of the statute,"[322] adding, "if [the Wiretap Act] does not apply extraterritorially, then government surveillance outside the United States is unconstrained, not forbidden, by [its terms]."[323] Albert Gidari has therefore argued that a U.S. court may conceivably authorize such a wiretap under the U.S.-UK Agreement using "any number of lesser forms of legal process," which would fall short of the protections the Wiretap Act mandates.[324] Precisely the same reasoning would apply to SCA orders.

V. CONCLUSION: IMPLICATIONS AND LINGERING QUESTIONS

This article has sought to inform the international community and others about the benefits and implications of direct access mechanisms, including but not limited to CLOUD Act agreements. Two main conclusions emerge. First, direct access mechanisms offer substantial international law benefits—at least in theory. Not only do they minimize conflicts—the main

321. *See* Albert Gidari, *More Questions About the CLOUD Act and the US-UK Agreement – Can the US Direct UK Providers to Wiretap Their Users in Third Countries?*, CTR. FOR INTERNET & SOC'Y (Nov. 13, 2019, 11:20 AM), http://cyberlaw.stanford.edu/blog/2019/11/more-questions-about-cloud-act-and -us-uk-agreement-can-us-direct-uk-providers-wiretap (arguing that the "listening post" approach to wiretap interception could potentially provide a rationale for U.S. interception of foreign transmissions).

322. United States v. Vega, 826 F.3d 514, 541 (D.C. Cir. 2016) (citing United States v. Chavez, 416 U.S. 580, 580 (1974)).

323. *Vega*, 826 F.3d at 541; *see* Gidari, *supra* note 321 ("Said another way, if the wiretap is extraterritorial, there is no Wiretap Act constraint in doing it."); *see also* United States v. Lugo Morales, No. 4:17-CR-203-ALM-KPJ, 2019 WL 1561901, at *2 (E.D. Tex. Mar. 21, 2019) (upholding a U.S. request for data from a foreign service provider, outside the SCA's scope, albeit on a voluntary basis).

324. Gidari, *supra* note 321. *See generally* Wiretap Act, 18 U.S.C. §§ 2510–23 (2018). The legality of this may depend on whether the request targeted U.S. persons or not. Existing authority suggests that extraterritorial U.S. law enforcement search and seizure targeting U.S. persons must comply with only the reasonableness requirement of the Fourth Amendment, not its warrant requirement. United States v. Stokes, 726 F.3d 880, 891–93 (7th Cir. 2013); *In re* Terrorist Bombings of U.S. Embassies in E. Afr., 552 F.3d 157, 167–73 (2d Cir. 2008); *c.f.* Kyllo v. United States, 533 U.S. 27, 31–35 (2001) (summarising the Fourth Amendment's warrant requirement). While a "lesser form of legal process" would appear permitted under the U.S.-UK Agreement, it may be unreasonable under the Fourth Amendment. *See* U.S.-UK AGREEMENT, *supra* note 2, arts. 1(1), 5(7)–(8) (permitting orders to be "subject to review or oversight . . . by a court, judge, or other independent authority prior to, *or in proceedings regarding*, enforcement of the order") (emphasis added). Orders targeting non-U.S. persons would not however be subject to the Fourth Amendment. United States v. Verdugo-Urquidez, 494 U.S. 259, 265–75 (1990).

stated benefit touted by the United States and United Kingdom when promoting the U.S.-UK Agreement—but they also provide states with the opportunity to expand enforcement jurisdiction extraterritorially against new service providers altogether.

Secondly, states should take seriously that these arrangements are reciprocal. The extent to which any given counterparty can take advantage of the international benefits outlined may turn on domestic law. However, contracting states should assume that the enhanced direct access one state gains to their counterpart's service providers will be met with commensurate direct access by that counterpart sovereign to the first state's own providers. While it is inevitable that international negotiations, including in the area of law enforcement assistance, operate based on trust,[325] this article has attempted to "pull back the curtain" by examining the United States' motivation and ability to directly use CLOUD Act agreements. The United States' statements to date, doubting that it would make much if any use of these agreements whatsoever, should be viewed critically: the United States has ample reasons to seek to use the U.S.-UK Agreement both to minimize conflicts and to expand jurisdiction—and its legal ability to do so as a matter of U.S. law appears, at minimum, far less restrained than it admits. Indeed, despite these public statements, it is clear that the United States is now devoting substantial resources precisely for the purposes of issuing CLOUD Act agreement requests.[326] For avoidance of doubt, while the United States' *White Paper* and similar statements are regrettable, there is nothing necessarily objectionable about the United States' motivation or ability to exercise such jurisdiction: it is, after all, precisely what the U.S.-UK Agreement contemplates and what the United Kingdom itself intends. States should, however, enter negotiations on the assumption that the reciprocity of these mechanisms matters.

A number of lingering questions remain. First, while this article's primary audience is foreign states operating on the international plane, its U.S., UK and EU law analysis highlights several issues for further domestic consideration. For the United States, the almost entirely unsettled nature of personal jurisdiction, both generally and in relation to the Fifth Amendment specifically, invites further study. Across the Atlantic, the UK's attempts to reform data protection law—particularly in a way that enables them to comply with the U.S.-UK Agreement's obligation to lift blocking statutes—will no doubt require extensive further consideration, including with regard to the ongoing relevance of the GDPR for service providers and others

325. See BOISTER, *supra* note 44, at 331–32.

326. *See* supra notes 224–225.

operating in the United Kingdom. This is likely to be merely one of a host of ongoing difficult legal issues resulting from Brexit that the United Kingdom (and the EU) will need to grapple with in the years ahead.

Much more analysis as to the benefits, risks, and operation of direct access mechanisms is also required. A particularly pressing task is unpacking further the consequences of reciprocity in the context of direct access. In at least some circumstances, allowing foreign state law enforcement direct access to compel data from domestic service providers may risk liability for a contracting state under international human rights law, as well as equivalent domestic provisions.[327] Equally, the extent to which *bilateral* direct access mechanisms can offer any long-term solution to the conflicts of law issues service providers increasingly face is unclear and worthy of further consideration. There is reason to doubt the ability of bilateral mechanisms to resolve what are, essentially, multilateral conflicts, as the example of the GDPR appears to indicate. A close eye should be kept on the developing EU and Budapest Convention proposals,[328] as well as a potential nascent United Nations treaty.[329] Overall, given the impact of reciprocity, coupled with these uncertainties, states should approach CLOUD Act agreements and similar mechanisms with caution.

327. *See, e.g.*, Bellia, *supra* note 107, at 99.

328. *See* COUNCIL OF EUROPE, *supra* note 26.

329. *See, e.g.*, Deborah Brown, *Cybercrime is Dangerous, but a New UN Treaty Could Be Worse for Rights*, JUST SECURITY (Aug. 13, 2021), https://www. justsecurity. org/ 77756/cybercrime-is-dangerous- but-a-new-un-treaty-could-be-worse-for-rights/ (expressing concerns that this proposed instrument may lead to foreign governments improperly gaining "direct access to massive amounts of information collected and stored by private companies").