Brooklyn Journal of International Law

Volume 47 | Issue 1 Article 1

12-1-2021

Digital Privacy Rights and CLOUD Act Agreements

Tim Cochrane

DIGITAL PRIVACY RIGHTS AND CLOUD ACT AGREEMENTS

*Tim Cochrane**

---

* Ph.D. Candidate, University of Cambridge Faculty of Law; M.Phil. Law (Dist.) (Oxon); LL.M. (Dist.) (UPenn); LL.B/B.A.(Hons.) (Otago); Attorney & Counselor-at-Law, New York State; Solicitor, Senior Courts of England and Wales; Barrister and Solicitor of the High Court of New Zealand (all currently non-practicing). This article was originally submitted as the author's M.Phil. thesis and was substantially updated while the author was in receipt of the Fitzwilliam College Stan Gold PhD Studentship. The author would like to thank Oliver Butler, Robert Currie, Anna Dannreuther, Liora Lazarus, and Kaiyi Xie for comments, as well as the journal staff for their patience and thoroughness. The usual disclaimers apply.

INTRODUCTION

The world is at a crossroads. On the one hand, swift access to data, often held overseas by companies like Google, Facebook and Amazon, is crucial for law enforcement investigations and prosecutions, but it is increasingly difficult to obtain. While data typically flows freely across borders, given its un-territorial nature,[1] the main tool law enforcement has to obtain overseas data—mutual legal assistance (MLA)[2]—is widely perceived to be ineffective, leading states to seek alternatives. On the other hand, there is growing recognition that law enforcement's access to data must be constrained by the important rights of privacy that people have over their data and devices—referred to throughout this article as "digital privacy rights." This article explores this tension, focusing on the United States (US) and United Kingdom's (UK) new proposed solution, CLOUD Act agreements.

CLOUD Act Agreements are named after their enabling US legislation, the Clarifying Lawful Overseas Use of Data Act 2018 (CLOUD Act).[3] Announcing the first bilateral CLOUD Act agreement in October 2019 (US–UK Agreement),[4] the US and UK stated that it would improve considerably on MLA, "while

1. *See generally* Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L. J. 326 (2015) [hereinafter Daskal, *Un-Territoriality*].

2. *See* NEIL BOISTER, AN INTRODUCTION TO TRANSNATIONAL CRIMINAL LAW 311–22 (2d ed. 2018); John A.E. Vervaele, *Mutual Legal Assistance in Criminal Matters to Control (Transnational) Criminality*, *in* ROUTLEDGE HANDBOOK OF TRANSNATIONAL CRIMINAL LAW 121, 121–36 (Neil Boister & Robert J. Currie eds., 2014) (both outlining mutual legal assistance [MLA]).

3. Clarifying Lawful Overseas Use of Data (CLOUD) Act, Pub. L. No. 115–141, 132 Stat. 348, div. V (2018) (codified in scattered sections of 18 U.S.C.) [hereinafter CLOUD Act].

4. *See* Agreement Between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, U.K.-U.S., Oct 3, 2019, Cm. 178 (U.K.) [hereinafter US–UK AGREEMENT].

protecting privacy and enhancing civil liberties."[5] Interrogating that claim, this article shows that the US–UK Agreement's impact on digital privacy rights will be more nuanced than currently acknowledged. In some respects, these rights will likely be enhanced. In other respects, however, they risk being undermined—and significantly so. The risk that CLOUD Act agreements will materially diminish rights should be taken seriously as it undermines the US and UK's stated rights-enhancing aims for CLOUD Act agreements.[6] To address this risk, this article argues for the US and UK to adopt a more sophisticated approach to the extraterritorial application of digital privacy rights in cross-border contexts of this nature.

Once in force,[7] the US–UK Agreement will allow US and UK law enforcement to directly enforce their own court orders for the preservation, interception, and disclosure of electronic data

---

5. Press Release, U.S. Dep't of Justice, U.S. and UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online (Oct. 3, 2019), https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists; *see* US–UK AGREEMENT, *supra* note 4, at art. 2(1); *see also* Press Release, White House Briefing Room, 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 ¶ 4 (June 10, 2021) [hereinafter JOINT STATEMENT] (stating that the US–UK Agreement is "based on a mutual recognition that both countries have an appropriately high level of data protection" and "maintain[] rigorous privacy standards"); Brian A. Benczkowksi, Assistant Att'y Gen., U.S. Dep't of Justice, Remarks at the 'Justice in Cyberspace' Symposium (Feb. 5, 2020) ("Our agreement with the U.K. is premised on both countries' appropriate protections of privacy and freedom.").

6. *See supra* text accompanying note 5. This is also reflected in the criteria the US sets for foreign states seeking CLOUD Act Agreements. *See* CLOUD Act § 105(a) (codified at 18 U.S.C. § 2523(b)(1) (2018)) (requiring that "domestic law of the foreign government, including the implementation of that law, [relevantly] affords robust substantive and procedural protections for privacy and civil liberties"); *see also* text accompanying *infra* notes 120–121.

7. *See* Commission Implementing Decision (EU) No. 2021/1772 of 28 June 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, C(2021) 4800, (153), https://ec.europa.eu/info/sites/info/files/draft_decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_19_feb_2020.pdf [hereinafter UK Adequacy Decision] (noting, as of Feb. 19, 2021, the United Kingdom and United States needed to resolve "details of the concrete implementation of the [agreement's] data protection safeguards" prior to its implementation).

extraterritorially against service providers in the other jurisdiction, bypassing MLA.[8] Taking a rights-based, comparative analysis, this article focuses on how this shift from MLA will impact the extent to which individuals have meaningful digital privacy rights, focusing on the core constitutional protections given to these rights by the Fourth Amendment of the US Constitution and Article 8 of the European Convention on Human Rights (ECHR).[9] Underlying this article are two related assumptions. First, rights, whether termed 'human rights' or 'constitutional rights'—including those within mechanisms such as the ECHR and US Constitution—should be taken seriously.[10] It argues that such rights should be at the forefront of analysis of CLOUD Act agreements and other methods to reform law enforcement cross-border data sharing. As noted, this assumption also appears to be an express aim of the US and UK's new US–UK Agreement. Second, these rights should be given universal effect insofar as possible—i.e. they should protect people whenever and wherever impacted, regardless of their nationality or location. While it is beyond the scope of this article to defend this notion of universality, it has strong normative justifications.[11] Universality is also "[the] driving force" behind various international human rights treaties, to which the US and UK are each a party.[12]

---

8. *See* STEPHEN P. MULLIGAN, CONG. RSCH. SERV., R45173, CROSS-BORDER DATA SHARING UNDER THE CLOUD ACT 19–20 (2018).

9. *See* Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 221 [hereinafter ECHR]. The ECHR is given direct UK effect through the Human Rights Act 1998, c.42 (U.K.) [hereinafter HRA].

10. *See generally* RONALD DWORKIN, TAKING RIGHTS SERIOUSLY (1997).

11. *See, e.g.*, Rep. of the Office of the U. N. High Comm'r for Hum. Rts., The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37, ¶ 8 (June 30, 2014) [hereinafter *The Right to Privacy in the Digital Age*]; Yuval Shany, *Taking Universality Seriously: A Functional Approach to Extraterritoriality in International Human Rights* Law, 7 L. & ETHICS HUM. RTS. 47 (2013); David Cole, *Are Foreign Nationals Entitled to the Same Constitutional Rights As Citizens?*, 25 T. JEFFERSON L. REV. 367 (2003); Bertrand G. Ramcharan, *The Universality of Human Rights*, *in* 58-59 INT'L COMMITTEE OF JURISTS REV. 105 (Adama Dieng ed., 1997); P (by his litigation friend the Official Solicitor) v. Cheshire West and Chester Council [2014] UKSC 19 [36] (Lady Hale), [2014] 1 AC 896 (appeal taken from Eng.) ("The whole point about human rights is their universal character.").

12. MARKO MILANOVIC, EXTRATERRITORIAL APPLICATION OF HUMAN RIGHTS TREATIES: LAWS, PRINCIPLES, AND POLICY 108 (2011); *e.g.*, International

This article provides the first in-depth analysis of the impact of CLOUD Act Agreements on digital privacy rights in both the US and UK,[13] as well as the first detailed consideration of how such new agreements will operate in practice. This analysis is invaluable for these States, as well as courts and others grappling with these agreements. Australia, for example, recently became the second country to sign a CLOUD Act Agreement with the US.[14] While this article focuses on the US–UK Agreement, it may nonetheless inform Australia's ongoing implementation of its own CLOUD Act agreement—indeed, concerns about rights similar to those explored here were raised repeatedly during legislative consideration of the Australian bill enacted to facilitate its entry into its new agreement.[15] This article may equally assist with consideration of other direct access regimes being developed around the world by the European Union (EU) and others.[16] More broadly, its recommendations may encourage rights-

---

Covenant on Civil and Political Rights, pmbl., Dec. 16, 1966, S. TREATY DOC. 95-20, 999 U.N.T.S. 171.

13. Other literature has provided brief or partial discussion of constitutional rights issues. *See, e.g.*, PETER SWIRE & JUSTIN HEMMINGS, AM. CONST. SOC'Y, OVERCOMING CONSTITUTIONAL OBJECTIONS TO THE CLOUD ACT (2020), https://www.acslaw.org/wp-content/uploads/2020/02/Overcoming-Constitutional-Objections-to-the-CLOUD-Act.pdf [hereinafter SWIRE & HEMMINGS, OVERCOMING] (discussing "potential facial and as-applied" Fourth Amendment challenges); Miranda Rutherford, *The CLOUD Act: Creating Executing Branch Monopoly over Cross-Border Data Access*, 34 BERKELEY TECH. L. J. 1177 (2019) (considering due process and other issues).

14. Press Release, U.S. Dep't of Justice, United States and Australia Enter CLOUD Act Agreement to Facilitate Investigations of Serious Crime (Dec. 15, 2021), https://www.justice.gov/opa/pr/united-states-and-australia-enter-cloud-act-agreement-facilitate-investigations-serious-crime; *see* Agreement Between the Government of Australia and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, Austl.-U.S., Dec. 15, 2021 (Austl.), https://www.homeaffairs.gov.au/nat-security/files/cloud-act-agreement-signed.pdf. [hereinafter US–AU AGREEMENT]

15. *E.g.*, Australian Parliamentary Joint Committee on Human Rights, Human Rights Scrutiny Report 9–26 (R4/2020, Apr. 9, 2020); Commonwealth, *Parliamentary Debates,* House of Representatives, 23 June 2021, 6904 (Adam Bandt MP); *see Telecommunications Legislation Amendment (International Production Orders) Act 2021* (Cth) (Austl.) [hereinafter TLAIPOA].

16. A recently finalized Second Additional Protocol to the Council of Europe [CoE] Cybercrime Convention, Computer Crime Convention Between the United States of America and Other Governments, Nov. 23, 2001, T.I.A.S. 13174, E.T.S. 185, expected to be open for signature in May 2022, will enable a direct access mechanism for certain data. Cybercrime Convention Committee

based reforms to MLA and other cross-border data sharing mechanisms.

Part I outlines the impetus and operation of CLOUD Act agreements, the methodology of this article, and the existing literature, which is currently deeply divided. While debate continues to evolve, positions are split broadly into two groups. On one side are US academics, who predominantly view CLOUD Act agreements as neutral or rights-enhancing, as states will be incentivized to improve their own laws to qualify for these agreements.[17] On the other side is a developing body of largely European literature expressing concerns that these new direct access mechanisms will severely undermine rights, including by removing MLA's safeguards.[18]

Part II compares the extent to which persons implicated by US and UK criminal investigations have effective digital privacy rights in practice when their data is sought through MLA with the comparative position they will be in when their data is obtained through CLOUD Act agreements. This analysis builds on existing literature analyzing MLA from a rights-based perspective.[19] It distinguishes between US persons, UK persons, and

---

(T-CY), Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-Operation and Disclosure of Electronic Evidence, CM(2021)57-final (Nov. 17, 2021); *see* Press Release, CoE, Cybercrime: Council of Europe Strengthens its Legal Arsenal (Nov. 17, 2021), https://search.coe.int/directorate_of_communications/Pages/result_details.aspx?ObjectId=0900001680a48ca6. The European Union [EU] is considering its own internal direct access mechanism, permitting direct access requests within EU member states. *See generally 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). UK legislation enabling the US–UK Agreement contemplates separate bilateral agreements between the United Kingdom [UK] and other states. *See* Crime (Overseas Production Orders) Act 2019, c.5, §§ 1, 4 (U.K.) [hereinafter COPOA]; Investigatory Powers Act 2016, c.25, § 52 (U.K.) [hereinafter IPA]. New Australian legislation is even broader, allowing multilateral "designated international agreement[s]." *See* TLAIPOA sch 1 item 3 (Austl.).

17. *See* discussion *infra* Section I.C.

18. *See id.*

19. *E.g.*, Tilmann Altwicker, *Transnationalizing Rights: International Human Rights Law in Cross-Border Contexts*, 29 EUR. J. INT'L L. 581, 594 (2018); Robert J. Currie, *The Protection of Human Rights in the Suppression of Transnational Crime*, *in* ROUTLEDGE HANDBOOK OF TRANSNATIONAL CRIMINAL LAW 27, 28 (Neil Boister & Robert J. Currie eds. 2015) [hereinafter Currie, *Protection*]; Robert J. Currie, *Human Rights and International Mutual Legal Assistance: Resolving the Tension*, 11 CRIM. L. F. 143, 144 (2000) [hereinafter Currie,

third country persons (TCPs). US and UK persons are terms used to describe citizens or permanent residents of their respective states, while all other persons—assumedly outside the physical territory of either the US or UK—are referred to as TCPs.[20] This article explains that, when the impact on rights is evaluated by distinguishing between these three groups of people, the diverging views in literature are each revealed as partly right and partly wrong. While the US–UK Agreement will likely be an overall relative improvement for the digital privacy rights of most US and UK persons,[21] it risks further undermining the already very limited digital privacy rights these States afford to TCPs.[22] This consequence flows from existing narrow judicial interpretations—already a problem for the protection of rights under MLA— limiting the bases of protection offered by the Fourth Amendment and Article 8 by nationality and geography, respectively.

Part III addresses what should be done. It argues that, for the rights-enhancing aims of CLOUD Act agreements to come true, each State should voluntarily extend the protections of the Fourth Amendment and Article 8, as applicable, to TCPs under the US–UK Agreement and any future direct access mechanisms. This step would give real force to these mechanisms' aims and therefore foster a cross-border law enforcement culture that better protects rights during trans-Atlantic data transfers.[23] It would also be readily achievable and, with a notable recent

---

Human Rights]; Maria Laura Ferioli, *Safeguarding Defendants' Rights in Transnational and International Cooperation*, *in* LEGAL RESPONSES TO TRANSNATIONAL AND INTERNATIONAL CRIMES: TOWARDS AN INTEGRATIVE APPROACH 203, 204 (Harmen van der Wilt & Christophe Paulussen eds., 2017); C. Gane & M. Mackarel, *The Admissibility of Evidence Obtained from Abroad into Criminal Proceedings – The Interpretation of Mutual Legal Assistance Treaties and Use of Evidence Irregularly Obtained*, 4 EUR. J. CRIME, CRIM. L. & CRIM. JUST. 98, 99 (1996); Aukje A.H. van Hoek & Michiel J.J.P. Luchtman, *Transnational Cooperation in Criminal Matters and the Safeguarding of Human Rights*, 1 UTRECHT L. REV., 1, 4 (2005).

20. *See infra* sources cited notes 125, 410 and accompanying text, discussing targeting restrictions under the US–UK Agreement. This article assumes that third country persons [TCPs] are outside the physical territory of either the US or UK at all times.

21. *See* discussion *infra* Sections II.B. and II.D.

22. *See* discussion *infra* Section II.E.

23. *See* discussion *infra* Section III.A.

exception,[24] be broadly consistent with judicial trends on the extraterritorial application of each of these mechanisms.[25] It would, moreover, significantly progress resolution of the ongoing problems stymying trans-Atlantic data transfers generally, as well as encouraging a more robust, rights-based approach to international data transfers across the globe.

I. CLOUD ACT AGREEMENTS AND THEIR INITIAL RECEPTION

A. The Impetus for and Operation of CLOUD Act Agreements

1. Criminal Investigations in the Digital Era

Rights are intimately engaged by criminal investigations.[26] They are seen to be in tension with concepts like security, truth, and justice.[27] States therefore adopt various *ex ante* and *ex post* mechanisms to balance rights and other societal interests.[28] *Ex ante*—in advance—methods include safeguards aimed at preventing breaches and minimizing their impact when they occur, such as requiring independent court approval of search warrants.[29] *Ex post*—after the fact—mechanisms comprise sanctions against law enforcement officials for misconduct and remedies for victims.[30] In particular, where evidence has been obtained in breach of rights, the most effective remedy will

---

24. Agency for Int'l Dev. v. All. for Open Soc'y Int'l, Inc., 140 S. Ct. 2082, 2086–87 (2020); *see* text accompanying notes 519–522.

25. *See* discussion *infra* Sections III.B and III.C.

26. DIMITRIOS GIANNOULOPOULOS, IMPROPERLY OBTAINED EVIDENCE IN ANGLO-AMERICAN AND CONTINENTAL LAW 208–11 (2019); STEFAN TRECHSEL, HUMAN RIGHTS IN CRIMINAL PROCEEDINGS 6–8 (2006).

27. *See* GIANNOULOPOULOS, *supra* note 26, at 28–44; TRECHSEL, *supra* note 26, at 6–8; Jenia Iontcheva Turner, *Regulating Interrogations and Excluding Confessions in the United States: Balancing Individual Rights and the Search for the Truth*, *in* DO EXCLUSIONARY RULES ENSURE A FAIR TRIAL?: A COMPARATIVE PERSPECTIVE ON EVIDENTIARY RULES 93, 94 (Sabine Gless & Thomas Richter eds., 2019).

28. GIANNOULOPOULOS, *supra* note 26, at 66, 251–52.

29. *Id.*; *e.g.* Sabine Gless & Laura Macula, *Exclusionary Rules – Is It Time for Change?*, *in* DO EXCLUSIONARY RULES ENSURE A FAIR TRIAL?: A COMPARATIVE PERSPECTIVE ON EVIDENTIARY RULES 349, 358–59, 363–66 (Sabine Gless & Thomas Richter eds., 2019); Turner, *supra* note 27, at 97.

30. GIANNOULOPOULOS, *supra* note 26, at 251–52; *e.g.* Gless & Macula, *supra* note 29, at 359–60, 367–75.

typically be *ex post*, through exclusion of that evidence during criminal proceedings.[31]

States have, however, struggled to effectively apply such rights in cross-border contexts.[32] This is increasingly significant in "the digital era,"[33] in which "[l]ives are increasingly lived online."[34] Data proliferates and flows freely across international borders,[35] and digital evidence is ubiquitous in criminal investigations.[36] Responding to this, US and UK law recognize that significant, perhaps "unique,"[37] privacy interests attach to searches

31. The classic exposition is Andrew Ashworth, *Excluding Evidence as Protecting Rights*, 1977 CRIM. L. REV. 723; *see also* Paul Roberts, *Excluding Evidence as Protecting Constitutional or Human Rights?*, *in* PRINCIPLES AND VALUES IN CRIMINAL LAW AND CRIMINAL JUSTICE: ESSAYS IN HONOUR OF ANDREW ASHWORTH 171 (Lucia Zedner & Julian V. Roberts eds., 2012) (revisiting Ashworth's thesis). *See generally* GIANNOULOPOULOS, *supra* note 26, at 200–54 (elaborating rights-based reasons to exclude evidence).

32. Altwicker, *supra* note 19, at 584–87; Currie, *Human Rights*, *supra* note 19, at 143, 171–78; *see* Currie, *Protection*, *supra* note 19, at 29–30, 38–39; *see also* Gane & Mackarel, *supra* note 19, at 105–08 (outlining "recurring problem[s]" with upholding rights in transnational criminal contexts).

33. *The Right to Privacy in the Digital Age*, *supra* note 111, ¶¶ 1–2.

34. Big Brother Watch v. U.K. [GC], App. No. 58170/13, ¶ 341 (May 25, 2021) http://hudoc.echr.coe.int/eng?i=001-210077.

35. Daskal, *Un-Territoriality*, *supra* note 1, at 366–68; Andrew Keane Woods, *Against Data Exceptionalism*, 68 STAN L. REV. 729, 758–60 (2016).

36. OFF. OF LEGAL EDUC. EXEC. OFF. FOR U.S. ATT'YS, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS ix (2009), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf (it is "important (and sometimes essential) evidence in criminal cases"); U.K. HOME OFFICE, CRIME (OVERSEAS PRODUCTION ORDERS) BILL 2018: OVERARCHING FACT SHEET 3 (2018), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/738076/2018-09-04_COPO_Detailed_Factsheet__final.pdf [hereinafter UK FACT SHEET] (it is "vital"); *see* Els de Busser, *EU-US Digital Data Exchange to Combat Financial Crime: Fast is the New Slow*, 19 GER. L. J. 1251, 1252 (2018) [hereinafter de Busser, *EU-US*] (it is "a new normal"); Jennifer Daskal, *Privacy and Security Across Borders*, 128 YALE L. J. F. 1029, 1032 (2019) [hereinafter Daskal, *Privacy and Security*] (it is "increasingly critical").

37. LAW COMMISSION, SEARCH WARRANTS, HC 852, ¶¶ 14.125–14.136 (2021) (UK).

and seizures of electronic data by law enforcement.[38] Similar trends are apparent in jurisdictions across the globe.[39]

The proliferation of electronic data across borders "presents both opportunities and challenges" for law enforcement.[40] Our data is now commonly held by third party service providers,[41] such as Google, Facebook, and Amazon. US and UK law enforcement often seek data for criminal investigations indirectly through such providers,[42] which are typically headquartered in the US[43] but may store data on servers around the world.[44] Law enforcement, however, has limited methods for obtaining data

---

38. Riley v. California, 573 U.S. 373, 393–401 (2014); Szabó & Vissy v. Hungary, App. No. 37138/14, ¶ 53 (Jan. 12, 2016), https://hudoc.echr.coe.int/fre?i=001-160020; *e.g.*, BC v. Chief Constable of the Police Serv. Of Scot. [2019] CSOH 48 [87], (2019) SLT 875 (Scot.), *aff'd on other grounds*, [2020] CSIH 61, (2021) SC 265 (Scot.).

39. *See* Lisl Brunner, *Digital Communications and the Evolving Right to Privacy*, *in* NEW TECHNOLOGIES FOR HUMAN RIGHTS LAW AND PRACTICE 217, 223–24 (Molly K. Land & Jay D. Aronson eds., 2018); RONALD J. KROTOSZYNSKI, JR., PRIVACY REVISITED: A GLOBAL PERSPECTIVE ON THE RIGHT TO BE LEFT ALONE 17, 117 (2016); *e.g.*, *AmaBhungane Centre for Investigative Journalism NPC v. Minister of Justice and Correctional Services* 2021 (3) SA 246 (CC) at paras. 1–2 (S.Afr.); R v. Marakah, 2017 SCC 59 paras. 33–37, [2017] 2 S.C.R. 608 (Can.); *Dotcom v. Att'y-Gen.* [2014] NZSC 199 [191], [2015] 1 NZLR 745 (N.Z.).

40. Robert J. Currie, *Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the* Microsoft Ireland *Case the "Next Frontier"?*, 54 CAN. Y.B. INT'L L. 63, 66 (2016) [hereinafter Currie, *Cross-Border*]; *see also* Jennifer Daskal, *Law Enforcement Access to Data Across Borders: the Evolving Security and Rights Issues*, 8 J. NAT'L SECURITY L. & POL'Y 473, 500 (2016) [hereinafter Daskal, *Law Enforcement Access*] ("The growing interest in access to data across borders provides a human rights opportunity, at the same time it poses a risk.").

41. DAVID ANDERSON, A QUESTION OF TRUST: REPORT OF THE INVESTIGATORY POWERS REVIEW ¶ 6.95 (2015), https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Web-Accessible1.pdf; Daskal, *Privacy and Security*, *supra* note 36, at 1033.

42. Daskal, *Privacy and Security*, *supra* note 36, at 1033; s*ee* OFF. OF LEGAL EDUC.*, supra* note 36, at 115–88 (listing U.S. methods for indirect access); UK FACT SHEET, *supra* note 36, at 3 (discussing UK methods); *see* Andrew Keane Woods, *Mutual Legal Assistance in the Digital Age*, *in* THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW 659, 660–61 (David Gray & Stephen E. Henderson eds., 2017) (detailing recent volumes of UK data requests for US service providers).

43. Woods, *supra* note 42, at 661–62, 663 n.9.

44. *See* Paul W. Schwartz, *Legal Access to the Global Cloud*, 118 COLUM. L. REV. 1681, 1686, 1689–99 (2018) (describing extraterritorial data storage methods of service providers).

beyond their borders, absent consent or access to a physical device containing it.[45] Overseas service providers will often refuse direct requests on the basis that providing the requested data would breach applicable "blocking statutes,"[46] such as the US Stored Communications Act (SCA) or the UK Investigatory Powers Act 2016 (IPA).[47] For example, the SCA generally prohibits disclosure of communications content—i.e. the full text of an email—although not non-content data, other than to US law enforcement.[48] In practice, service providers may be even stricter, refusing all foreign requests.[49]

When direct requests by a foreign state are made unilaterally and under threat of compulsion, they are also commonly perceived to breach the customary international law prohibition against unilateral extraterritorial enforcement jurisdiction.[50] A

---

45. *See* OFF. OF LEGAL EDUC., *supra* note 36, at 56–59; UK FACT SHEET, *supra* note 36, at 3; *see* Jay V. Prabhu, Alexander P. Berrang & Ryan K. Dickey, *When Your Cyber Case Goes Abroad: Solutions to Common Problems in Foreign Investigations*, *in* 67 DEP'T OF JUST. J. FED. L. & PRAC. 167, 177–79 (2019) (discussing this challenge and potential US law enforcement options); LAW COMMISSION, *supra* note 37, ¶¶ 14.32–14.112 (similarly outlining UK options).

46. Woods, *supra* note 42, at 662–63; Jennifer Daskal, *Borders and Bits*, 71 VAND. L. REV. 179, 195–98 (2018) [hereinafter Daskal, *Borders and Bits*].

47. Stored Communications Act, Pub. L. No. 99–508, tit. II, 100 Stat. 1848, 1860–68 (1986) (codified as amended at 18 U.S.C. §§ 2701–13 (2018)) [hereinafter SCA]; IPA, §§ 3, 11; *see* 164 CONG. REC. S1923 (daily ed. Mar. 22, 2018) (statement of Sen. Hatch) (referring to the SCA as a "blocking statute"); HL Deb (20 Nov. 2018) (794) col. 140 (UK) (referring to the IPA similarly).

48. SCA, 18 U.S.C. § 2702(a) (2018); *see* Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PENN. L. REV. 373, 378–85 (2014).

49. ANDERSON, *supra* note 41, ¶¶ 9.74, 11.18; Kate Westmoreland, *Are Some Companies "Yes Men" When Foreign Governments Ask for User Data?*, CTR. FOR INTERNET & SOC'Y (May 30, 2014, 1:12 PM), http://cyberlawhttp://cyberlaw.stanford.edu/blog/2014/05/are-some-companies-yes-men-when-foreign-governments-ask-user-data; *e.g.*, *Transparency at Dropbox – Reports*, DROPBOX, https://www.dropbox.com/transparency/reports (last visited Feb. 16, 2022) (follow "Location" hyperlink; then follow "International" hyperlink) ("[W]e typically require non-US governments to follow the Mutual Legal Assistance Treaty [MLAT] process or letters rogatory process"); *see* Woods, *supra* note 42, at 662–63 (noting "confusion about" blocking statutes allow US service providers "coyly to resist law enforcement demands even when there is no clear legal barrier").

50. *E.g.*, BOISTER, *supra* note 2, at 328–30; Currie, *Cross-Border*, *supra* note 40, at 93–94; Daskal, *Un-Territoriality*, *supra* note 1, at 390–91. *But see* LAW COMMISSION, *supra* note 37, ¶¶ 16.67–16.69, 16.94 (discussing a "lack of clarity"). For a general overview, *see* Michael Akehurst, *Jurisdiction in International Law*, 46 BRIT. Y. B. INT'L. L. 145, 146–48 (1972-1973) (outlining this

state acts 'extraterritorially' when they act outside their territory.[51] International law distinguishes between *prescriptive* jurisdiction—the ability to make laws about particular matters—and *enforcement* jurisdiction—the ability to actually enforce or apply these laws.[52] While international law takes a "generally permissive approach" to extraterritorial prescriptive jurisdiction, enforcement jurisdiction has traditionally been seen as "strictly territorially bounded,"[53] absent consent from the foreign state whose territory is implicated.[54] To the extent it remains in force, certain State conduct, including the recent US and UK conduct outlined below, arguably breaches this prohibition.[55] The continued existence of this prohibition, particularly in the digital arena, has recently been described as "unclear."[56]

2. Mutual Legal Assistance (MLA), Human Rights, and 'the MLAT Problem'

MLA is often the only method available to law enforcement to obtain overseas data.[57] It operates through multilateral conventions, bilateral treaties (MLATs) and, absent those,

---

aspect of international law); Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. Rep. 244 (Dec. 15); S.S. Lotus (Fr. V. Turk.), Judgment, 1927 P.C.I.J. (ser. A) No. 10, at 18–19 (Sept. 7); BOISTER, *supra* note 2, at 281–283; Currie, *Cross-Border*, *supra* note 40, at 69–74.

51. Currie, *Cross-Border*, *supra* note 40, at 69.

52. *Id.* at 70.

53. *Id*; *see* Stephen W. Smith, *Clouds on the Horizon: Cross-Border Surveillance Under the US CLOUD Act*, *in* DATA PROTECTION BEYOND BORDERS: TRANSATLANTIC PERSPECTIVES ON EXTRATERRITORIALITY AND SOVEREIGNTY 119, 122 (Federico Fabbrini, Edoardo Celeste & John Quinn eds., 2020).

54. JAMES CRAWFORD, BROWNLIE'S PRINCIPLES OF PUBLIC INTERNATIONAL LAW 462 (9th ed. 2019).

55. *See* Currie, *Cross-Border*, *supra* note 40 80–93; Daskal, *Borders and Bits*, *supra* note 46, at 186–198.

56. LAW COMMISSION, *supra* note 37, ¶¶ 16.94–16.100; Smith, *supra* note 53, at 133; *e.g.* R (KBR, Inc.) v. Dir. of the Serious Fraud Office [2021] UKSC 2 [51], [2021] 2 WLR 335 (appeal taken from Eng.) (noting uncertainty). *But see also* Currie, *Cross-Border*, *supra* note 40, at 94 (concluding in 2016 that the prohibition remained in force based on a survey of state practice). *See generally* Stephen Allen, *Enforcing Criminal Jurisdiction in the Clouds and International Law's Enduring Commitment to Territoriality*, *in* THE OXFORD HANDBOOK OF JURISDICTION IN INTERNATIONAL LAW 381 (Stephen Allen, Daniel Costelloe, Malgosia Fitzmaurice, Paul Gragl & Edward Guntrip eds., 2019).

57. Woods, *supra* note 42, at 659; *e.g.*, OFF. OF LEGAL EDUC., *supra* note 36, at 56–57; UK FACT SHEET, *supra* note 36, at 3.

understandings of comity.[58] The US and UK have a close MLA relationship,[59] operating both informally, through "police-to-police cooperation,"[60] and formally through an MLAT in force since 1996 (US–UK MLAT).[61] Requests to the US or UK for electronic content data held by service providers require formal MLA, as compulsory legal processes are normally required to obtain such data.[62] As a requesting state is not itself acting extraterritorially, MLA respects the prohibition against unilateral extraterritorial enforcement jurisdiction.[63] Since MLA requests typically must comply with the laws of both requesting and requested states, MLA has been described as providing a "built-in-system of double control" and a "double check" for rights, because targets theoretically benefit from the protections of two legal systems.[64]

There are however two core problems with using MLA to obtain overseas electronic data. First, while MLA may in theory provide a "double check" for rights, it more commonly functions as a "double-edged sword:" while states provide broad assistance for law enforcement internationally, it is in a context in which

---

58. Vervaele, *supra* note 2, at 122.

59. R (Terra Servs.' Ltd.) v. National Crime Agency [2019] EWHC (Admin) 3165 [16]–[17], [2020] Lloyd's Rep. F.C. 29.

60. *See* BOISTER, *supra* note 2, at 308.

61. Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-U.K., Jan. 6, 1994, T.I.A.S. No. 96–1202 [hereinafter US–UK MLAT]; *see also* Instrument Amending the Treaty on Mutual Legal Assistance in Criminal Matters, Dec. 16, 2004, T.I.A.S. No. 10-201.49. (updating the US–UK MLAT to reflect a related US–EU instrument).

62. *See* BOISTER, *supra* note 2, at 311.

63. Allen, *supra* note 56, at 385; BOISTER, *supra* note 2, at 311; *see* de Busser, *EU-US*, *supra* note 36, at 1255–56 ("The backbone of [MLA] is territorial sovereignty").

64. Lawrence Siry, *Cloudy Days Ahead: Cross-border Evidence Collection and its Impact on the Rights of EU Citizens*, 10 NEW J. EUR. CRIM. L. 227, 232, 250 (2019); *see* Christine Galvagna, *The Necessity of Human Rights Legal Protections in Mutual Legal Assistance Treaty Reform*, 9 NOTRE DAME J. INT'L & COMP. L. 57, 65–66 (2019) (arguing that MLA data requests provide "effective legal protections"); Halefom H. Abraha, *How Compatible is the US 'CLOUD Act' with Cloud Computing? A Brief Analysis*, 9 INT'L DATA PRIV. L. 207, 213 (2019) ("The rigorous procedures in the MLAT system are important safeguards for privacy and due process"); Robyn Greene, *Four Common Sense Fixes to the CLOUD Act that its Sponsors Should Support*, JUST SECURITY (Mar. 13, 2018), https://www.justsecurity.org/53728/common-sense-fixes-cloud-act-sponsors-support/ ("The MLAT process is a rights-respecting process").

protections for rights are diminished or ignored altogether.[65] As Robert Currie explains, the internationalization of criminal law through MLA historically developed in "splendid isolation" from human rights, which largely remain territorially bounded in the eyes of states.[66] In 1989 the European Court of Human Rights (ECtHR) recognized that ECHR member states must not extradite in breach of ECHR rights in *Soering v. United Kingdom*.[67] Although extradition is a form of MLA,[68] this principle has not yet been expanded to MLA generally.[69]

MLA therefore leads to "protection gaps."[70] As set out in Part 2, MLA as practiced by the US and UK involves fewer *ex ante* and, most significantly, *ex post* rights protections than equivalent methods used to obtain data domestically.[71] Most strikingly, these states rely on what has been called the "rule of non-

65. Currie, *Protection*, *supra* note 19, at 30; *see* Ferioli, *supra* note 19, at 205 ("[MLA] has traditionally paid little attention to the individual rights affected"); Els de Busser, *The Digital Unfitness of Mutual Legal Assistance*, 28 SEC. & HUM. RTS. 161, 168 (2017) [hereinafter de Busser, *Digital Unfitness*] ("The [MLA] grounds for refusal have not been drawn up out of a concern for the safeguarding of individuals' human rights."); *see also* Altwicker, *supra* note 19, at 584, 594 (discussing new hybrid forms of MLA, and cautioning that "[t]he human rights impact of these new types of [MLA] cooperation is often neglected."); Robert J. Currie, *Charter Without Borders? The Supreme Court of Canada, Transnational Crime and Constitutional Rights and Freedoms*, 27 DALHOUSIE L. J. 235, 284 (2004) [hereinafter Currie, *Charter Without Borders?*] (critiquing the view that "the pressing and substantial need for [MLA] justifies a looser approach to how the state will be held to the constitutional human rights standings imposed on it").

66. Currie, *Protection*, *supra* note 19, at 35.

67. Soering v. United Kingdom, 161 Eur. Ct. H.R. (ser. A) ¶¶ 85–91 (1989*)*.

68. CLIVE NICHOLLS, CLARE MONTGOMERY, JULIAN B. KNOWLES, ANAND DOOBAY & MARK SUMMERS, NICHOLLS, MONTGOMERY, AND KNOWLES ON THE LAW OF EXTRADITION AND MUTUAL ASSISTANCE ¶ 17.01 (3d ed. 2013).

69. Elgizouli v. Sec'y of State for the Home Dep't [2020] UKSC 10 [68] (Lord Kerr dissenting but not on this point), [2021] AC 937 (appeal taken from Eng.); *see* Ferioli, *supra* note 19, at 208.

70. Ferioli, *supra* note 19, at 205; *see* KRIT ZEEGERS, INTERNATIONAL CRIMINAL TRIBUNALS AND HUMAN RIGHTS LAW: ADHERENCE AND CONTEXTUALIZATION 136–37 (2016); van Hoek & Luchtman, *supra* note 19, at 21; Currie, *Human Rights*, *supra* note 19, at 173–74, 176; *e.g.*, Currie, *Charter Without Borders?, supra* note 65, at 280 (discussing the Canadian context); Altwicker, *supra* note 19, at 584–87 (discussing "protection gaps" arising from related extraterritorial state conduct). *See generally* Shany, *supra* note 11, at 57 (referring to the "elimination" of "extraterritorial legal 'black holes'" as an aspect of "the constitutive ethos" of international human rights).

71. *See* discussion infra Sections II.A and II.C.

inquiry" to refuse to address credible allegations that rights have been breached by the other state during MLA.[72] This is compounded by the inherent difficulties targets face in gathering evidence of breaches internationally.[73] Further, to the extent the *Soering* principle is applicable to MLA, it is triggered only where there are "flagrant denials" of rights, and thus still allows for a reduction in protection.[74]

The second problem is the "slow and cumbersome" nature of MLA,[75] a concern "haunting [MLA] procedures for decades."[76] The UK estimates MLA requests to the US take a year or more.[77] The apparent difficulty of using MLA for electronic data is so widespread it is often referred to as "the MLAT problem."[78] It is attributed to various causes, including perceived insufficient MLA resource investments made by the US.[79] The MLAT

72. Ferioli, *supra* note 19, at 205–07; Currie, *Human Rights*, *supra* note 19, at 173–77; van Hoek & Luchtman, *supra* note 19, at 2–3. Ferioli describes the "rule of non-inquiry" in the context of MLA as meaning that a requested state "must assume that the requested state has collected the evidence in a lawful manner and declare it admissible." Ferioli, *supra* note 19, at 207.

73. *See* van Hoek & Luchtman, *supra* note 19, at 20; Currie, *Human Rights*, *supra* note 19, at 170.

74. Ferioli, *supra* note 19, at 208; *see* Sabine Gless, *Transnational Cooperation in Criminal Matters and the Guarantee of a Fair Trial: Approaches to a General Principle*, 9 UTRECHT L. REV. 90, 102–03 (2013) ("[T]he *Soering* doctrine is primarily a sort of 'fair trial emergency brake'").

75. *E.g.*, LAW COMMISSION, *supra* note 37, ¶ 16.146; RICHARD A. CLARKE, MICHAEL J. MORELL, GEOFFREY R. STONE, CASS R. SUNSTEIN & PETER SWIRE, LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES 226–27 (2013).

76. de Busser, *EU-US*, *supra* note 36, at 1259.

77. UK FOREIGN & COMMONWEALTH OFFICE, EXPLANATORY MEMORANDUM TO THE AGREEMENT BETWEEN THE GOVERNMENT OF THE UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND AND THE GOVERNMENT OF THE UNITED STATES OF AMERICA ON ACCESS TO ELECTRONIC DATA FOR THE PURPOSE OF COUNTERING SERIOUS CRIME, 2019, ¶ 2 [hereinafter UK EXPLANATORY MEMORANDUM].

78. *See* Gail Kent, *The Mutual Legal Assistance Problem Explained*, CTR. FOR INTERNET & SOC'Y (Feb. 23, 2015, 1:06 PM), http://cyberlaw.stanford.edu/blog/2015/02/mutual-legal-assistance-problem-explained; Currie, *Cross-Border*, *supra* note 40, at 83. This perception—that MLA is inherently inefficient for obtaining electronic data—is however disputed. Sergi Vazquez Maymir, *Anchoring the Need to Revise Cross-Border Access to E-Evidence*, 9 INTERNET POL'Y REV., 1, 9–11 (2020), https://doi.org/10.14763/2020.3.1495.

79. CLARKE, MORELL, STONE, SUNSTEIN & SWIRE, *supra* note 75, at 227–28; Bruce Zagaris, *U.S. Government's Ability to Obtain and Provide International Enforcement Constrained By Budget, Failure to Meet International Standards,*

problem is exacerbated by the evolving ways in which electronic data is stored, making it difficult, if not impossible, to know where to direct requests.[80] Its significance is further heightened by the ever-growing importance of electronic data for criminal investigations.[81]

3. Attempts to Solve the MLAT Problem

The MLAT problem—rather than MLA's failings to protect human rights—has led to various calls for reform.[82] While it is beyond the scope of this article to canvas all reforms, two linked US and UK reforms are directly relevant.

First is the CLOUD Act agreement model itself, which the US and UK began negotiating in the middle of the last decade.[83] Concerns with the MLAT problem are long-standing.[84] Nonetheless, the CLOUD Act's 'direct access' agreement model, by which states seek data directly from overseas service providers, appears to have been first proposed only in 2015 by Sir Nigel Sheinwald, then the UK's special envoy on intelligence and law enforcement data sharing, following discussions with overseas service providers and US law enforcement.[85] Along with MLA

---

and Join International Initiatives, 31 INT'L ENF'T L. REP. 514, 514 (2015); *see* Woods, *supra* note 42, at 664–66 (elaborating on these financial constraints).

80. Currie, *Cross-Border*, *supra* note 40, at 82–83 and 82 n.75; *see* Schwartz, *supra* note 44, at 1694–99 (articulating "a taxonomy of cloud types" used for data storage).

81. *See* Woods, *supra* note 42, at 664–66 ("[T]he number of cross-border requests for data is already enormous, and is poised to increase.").

82. *E.g.*, Peter Swire & Justin D. Hemmings, *Mutual Legal Assistance In an Era of Globalized Communications: The Analogy To the Visa Waiver Program*, 71 N.Y.U. ANN. SURV. AM. L. 687, 715–38 (2017) [hereinafter Swire & Hemmings, *Visa Waiver*]; Woods, *supra* note 42, at 663–73; *see also* Daskal, *Law Enforcement Access*, *supra* note 40, at 476–78 (summarizing state attempts to "facilitate direct access to sought-after data").

83. NICOLA NEWSOM, HOUSE OF LORDS LIBRARY, CRIME (OVERSEAS PRODUCTION ORDERS) BILL [HL]: BRIEFING FOR LORDS STAGES (July 5, 2018) (UK), https://researchbriefings.files.parliament.uk/documents/LLN-2018-0076/LLN-2018-0076.pdf; *see also* https://lordslibrary.parliament.uk/research-briefings/lln-2018-0076/.

84. *See* de Busser, *EU-US*, *supra* note 36, at 1259; *e.g.*, CLARKE, MORELL, STONE, SUNSTEIN & SWIRE, *supra* note 75, at 226–29; *cf.* Woods, *supra* note 42, at 660 (suggesting in 2017 concerns had then increased markedly from "even ten years ago").

85. UK CABINET OFFICE, SUMMARY OF THE WORK OF THE PRIME MINISTER'S SPECIAL ENVOY ON INTELLIGENCE AND LAW ENFORCEMENT DATA SHARING – SIR NIGEL SHEINWALD (2015). For background, see NICK CLEGG, POLITICS: BETWEEN

reform, Sir Nigel suggested "allow[ing] certain democratic countries—with similar values and high standards of oversight, transparency and privacy protection—to gain access to content in serious crime and counter-terrorism cases through direct requests to companies."[86] This was supported and expanded over several years by US academics, primarily Peter Swire, Jennifer Daskal, and Andrew Keane Woods.[87] These developments have occurred alongside debates in the EU and elsewhere, where similar direct access mechanisms are under consideration.[88] These mechanisms also have analogies with existing intelligence sharing tools used by the US, EU, and others.[89]

In the same period, the US and UK have also attempted "unilateral assertions of extraterritorial jurisdiction," by claiming their domestic laws can be used to compel disclosure of overseas data without recourse to MLA.[90] Whether particular SCA powers, which were silent as to their territorial scope, could be used to compel Microsoft to disclose data stored in Ireland was famously the subject of the US Second Circuit Court of Appeals' decision in *Microsoft Ireland*.[91] In the UK, powers in the IPA and

---

THE EXTREMES 111–13 (2016); ANDERSON, *supra* note 41, ¶ 11.27; *see also* Richard W. Downing, Deputy Assistant Att'y Gen., Remarks at the Academy of European Law Conference, 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 ("The impetus for the CLOUD Act came from our foreign law enforcement partners . . . The [UK]'s concerns in particular spurred our development of the CLOUD Act.").

86. CABINET OFFICE, *supra* note 85; *see also* ANDERSON, *supra* note 41, at 289 (offering similar recommendations).

87. *E.g.*, Swire & Hemmings, *Visa Waiver*, *supra* note 82, at 720, 725–38; Jennifer Daskal & Andrew Keane Woods, *Cross-Border Data Requests: A Proposed Framework*, LAWFARE (Nov. 24, 2015, 8:00 AM), https://www.lawfareblog.com/cross-border-data-requests-proposed-framework; NYU School of Law, *Symposium on Gov't Access to Data in the Cloud – 5*, YOUTUBE (May 29, 2015), https://www.youtube.com/watch?v=0U5WOYNQCaQ (Panel 5: Extraterritorial Application of U.S. Law to the Cloud, Panelists: Jennifer Daskal, Peter Swire, Andrew Woods & Michael Farbiarz).

88. *See supra* sources cited note 16 and accompanying text.

89. *See* Francesca Bignami & Giorgio Resta, *Transatlantic Privacy Regulation: Conflict and Cooperation*, 78 L. & CONTEMP. PROBS. 231, 241–47 (2015).

90. Daskal, *Law Enforcement Access*, *supra* note 40, at 477–78; *see* Currie, *Cross-Border*, *supra* note 40, at 91–93.

91. Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.), 829 F.3d 197 (2d Cir. 2016) [hereinafter *Microsoft Ireland*], *cert. granted sub nom.*, United

preceding legislation purport to be expressly extraterritorial,[92] although these have yet to be tested in court.[93] Attempts to apply UK statutory powers that were silent as to territorial scope extraterritorially initially met with greater success before UK courts.[94] In February 2021, however, the UK Supreme Court overturned the leading judgment, *KBR*,[95] holding that it was "inherently improbable" that the UK Parliament had intended such legislation to apply extraterritorially in this way.[96] A parliamentary preference for MLA was instead shown through "successive Acts of Parliament," the Court held.[97]

These two approaches to addressing the MLAT problem have progressed together; indeed, the primary effect of CLOUD Act agreements is to enable its members to apply their own domestic

---

States v. Microsoft Corp., 138 S. Ct. 356 (2017), *vacated as moot*, 138 S. Ct. 1186 (2018). *See generally* Justin Hemmings, Sreenidhi Srinivasan & Peter Swire, *Defining the Scope of "Possession, Custody, or Control" for Privacy Issues and the CLOUD Act*, 10 J. NAT'L SECURITY L. & POL'Y 631, 646–52 (2020).

92. *E.g.*, IPA §§ 9, 41-43, 85, 97, 139; *see* LAW COMMISSION, *supra* note 37, ¶ 16.84; ANDERSON, *supra* note 41, ¶¶ 6.95–6.98 (citing Data Retention and Investigatory Powers Act 2014, c.27, § 4 (U.K.) [hereinafter DRIPA]).

93. ANDERSON, *supra* note 41, ¶ 6.99.

94. *E.g.*, R (Jimenez) v. First Tier Tribunal (Tax Chamber) [2019] EWCA (Civ) 51, [31]–[49], [2019] 1 WLR 2956 (Eng.); R (KBR, Inc.) v. Dir. of the Serious Fraud Off. [2018] EWHC (Admin) 2368, [63]–[78], [2019] QB 675 (Eng.), *vacated* [2011] UKSC 2. For background, see LAW COMMISSION, *supra* note 37, ¶ 10.125; Alex Davidson, *Extraterritoriality and Statutory Interpretation: The Increasing Reach of Investigative Powers*, 1 PUB. L. 1, 1 (2020).

95. *See KBR, Inc.* [2018] EWHC (Admin) 2368, *vacated* [2021] UKSC 2 (Eng.).

96. R (KBR, Inc.) v. Dir. of the Serious Fraud Off. [2021] UKSC 2 [45], [2021] 2 WLR 335 (Eng.); *see* Tim Cochrane, *The Presumption Against Extraterritoriality, Mutual Legal Assistance, and the Future of Law Enforcement Cross-Border Evidence Collection*, 85 MOD. L. REV. 526 (2022) [hereinafter Cochrane, *The Presumption Against Extraterritoriality*] (elaborating on this conclusion), https://doi.org/10.1111/1468-2230.12675; *see also* Tim Cochrane, *KBR v. SFO: the United Kingdom's Microsoft Ireland?,* JUST SECURITY (Feb. 25, 2021) https://wwwhttps://www.justsecurity.org/74875/kbr-v-sfo-the-united-kingdoms-microsoft-ireland/ (discussing similarities and differences between the two judgments).

97. *KBR, Inc.* [2021] UKSC 2 [39]–[45] (referring to Criminal Justice Act 1988, c.33, § 29 (U.K.), Criminal Justice (International Co-operation) Act 1990, c.5 (U.K.), Criminal Justice and Public Order Act 1994, c.33 (U.K.), and Crime (International Co-operation) Act 2003, c.32 (U.K.) [hereinafter CICA]); *see* Cochrane, *The Presumption Against Extraterritoriality*, *supra* note 96, at 531–533 (elaborating).

laws extraterritorially.[98] In 2016, *Microsoft Ireland* held that compelling disclosure of Irish data would be an unlawful extraterritorial assertion of SCA powers, contrary to the underlying privacy focus of that legislation.[99] The very next day, the US Department of Justice (DOJ) submitted a draft of the CLOUD Act to Congress.[100] Although this draft was not initially progressed, calls for a legislative solution were raised by the Supreme Court during oral argument of an appeal of *Microsoft Ireland* in February 2018, as well as by Microsoft itself.[101] In response, on March 23, 2018, Congress enacted the CLOUD Act as part of a consolidated appropriations bill with little debate.[102]

CLOUD Act agreements have two major components.[103] The first gives express extraterritorial scope to the SCA.[104] The second creates the mechanism for international 'CLOUD Act' agreements.[105] Companion legislation, the Crime (Overseas Production Orders) Act 2019 (COPOA), was enacted by the UK

98. *See infra* sources cited note 116.

99. *Microsoft Ireland,* 829 F.3d at 216–21 (2d Cir. 2016). *Contra KBR, Inc.* [2021] UKSC 2 [30] ("[I]t is questionable whether in the hypothetical situation [i.e. *Microsoft Ireland*] the legislation is given any material extra-territorial effect.").

100. Letter from Peter J. Kadzik, U.S. Assistant Att'y Gen., to the Hon. Joseph R. Biden, President of the U.S. Senate (July 15, 2016), http://www.netcaucus.org/wp-content/uploads/2016-7-15-US–UK-Legislative-Proposal-to-Hill.pdf; *see* Letter from Samuel R. Ramer, Acting Assistant Att'y Gen., to Paul Ryan, Speaker of the U.S. House of Representatives (May 24, 2017), https://republicans-judiciary.house.gov/wp-content/uploads/2017/06/Downing-Testimony.pdf (Navigate to Appendix A at 18–35 of this PDF) (a similar letter sent the following year).

101. *See* Hemmings, Srinivasan & Swire, *supra* note 91, at 650–52.

102. *See, e.g.*, 164 CONG. REC. H1764–65 (daily ed. March 22, 2018) (statement of Rep. Hoyer) (complaining, in reference to the appropriations bill containing the CLOUD Act, "the real problem is that nobody knows what is in this legislation"); *see also* Schwartz, *supra* note 44, at 1751 ("At a minimum, these dramatic policy developments deserved greater scrutiny than being buried in a nearly thousand-page budget bill.").

103. *See generally* Halefom H. Abraha, *Regulating Law Enforcement Access to Electronic Evidence Across Borders: the United States Approach*, 29 INFO. & COMM. TECH. L. 324 (2020) (elaborating on these two aspects of CLOUD Agreements).

104. *See* CLOUD Act § 103(a)(1) (codified at 18 U.S.C. § 2713 (2018)).

105. *See id.* § 105(a) (codified at 18 U.S.C. § 2523 (2018)).

Parliament in February 2019,[106] again with limited debate.[107] Finally, in October 2019, the US and UK signed the US–UK Agreement, which may now come into force at any point through an exchange of diplomatic notes.[108]

4. CLOUD Act Agreements and Digital Privacy Protections

The main aspects of CLOUD Act agreements can be briefly stated.[109] First, as noted above, law enforcement currently face both practical limitations—resistance from providers—and risk breaching international law when attempting to compel data from overseas providers.[110] CLOUD Act agreements attempt to address this. "One of the core obligations of the [US–UK] agreement [is] the removal of any legal barriers that would prevent a UK [service provider] complying with a request from the US."[111] As it is reciprocal, the US–UK Agreement also obliges equivalent legal barriers preventing US providers complying with UK requests to be lifted.[112] This should go some way to addressing service providers' practical concerns that they would breach, for

106. *See* COPOA, pmbl.

107. *See, e.g.*, HL Deb (20 Nov. 2018) (794) col. 142 (UK) ("[T]he Bill has not exactly held this House in rapt attention, judging by the number of people who decided to participate in our debates.").

108. US–UK AGREEMENT, *supra* note 4, at art. 16; *see supra* text accompanying note 5.

109. *See supra* Part II (detailing the operation of CLOUD Act agreement requests specifically). As set out, the provisions outlined in this section appear also appear in the US–AU Agreement and are thus likely core attributes of the CLOUD Act agreement model.

110. *See supra* text accompanying notes 46–49.

111. HL Deb (20 Nov. 2018) (794) col. 140 (U.K.); U.S. DEP'T OF JUSTICE, PROMOTING PUBLIC SAFETY, PRIVACY, AND THE RULE OF LAW AROUND THE WORLD: THE PURPOSE AND IMPACT OF THE CLOUD ACT 4 (2019) [hereinafter US WHITE PAPER]; UK EXPLANATORY MEMORANDUM, *supra* note 77, ¶ 8; *see also* sources cited *infra* note 116.

112. *See* HL Deb (20 Nov. 2018) (794) col. 140 (U.K.); *see also* CLOUD Act § 105(b)(4)(I) (codified at 18 U.S.C. § 2523(b)(1) (2018)) (noting, as a condition of CLOUD Act agreements, that "the foreign government shall afford reciprocal rights of data access"); US–UK Agreement, *supra* note 4, at art. 2(3)(b) ("[T]he interest of each Party in being able to obtain electronic data pursuant to [the US–UK] Agreement requires them to provide the same ability to the other Party"); US–AU AGREEMENT, *supra* note 14, at art. 2 (similar).

example, US law by responding to a UK law enforcement request.[113]

By lifting domestic legal barriers, CLOUD Act agreements also purport to provide the required consent at the level of international law, permitting the UK to expand its enforcement jurisdiction over US service providers, and vice versa.[114] In this way, CLOUD Act agreements are "premised on consent."[115] The intent of their members is that requests to overseas service providers will now be solely dealt with under the law of the requesting state and by its authorities.[116] While nothing in CLOUD Act agreements directly compel providers to respond to requests, they build from an assumption that their members "will have the authority under their domestic laws to compel production of data held abroad."[117] Requests may therefore be compelled through the law of the requesting state, which are given practical extraterritorial force through these agreements.[118]

---

113. *See supra* text accompanying notes 46–49; *see also infra* text accompanying note 159–160 (noting that CLOUD Act agreements have the support of global service providers).

114. *See supra* text accompanying notes 50–56; *see also* Tim Cochrane, *Hiding in the Eye of the Storm Cloud: How CLOUD Act Agreements Expand U.S. Investigatory Powers*, 32 DUKE J. COMP. INT'L L. 153, 169–175, 181–189 (2021) (evaluating the impact of CLOUD Act agreements at international law).

115. Jennifer Daskal, *Transnational Government Hacking*, 10 J NAT'L SEC'Y L. & POL'Y 677, 695 (2020) [hereinafter Daskal, *Hacking*].

116. *See* US–UK AGREEMENT, *supra* note 4, at arts. 3(2), 5(1), 5(2), 8(1), 10(2), 10(5); US–AU AGREEMENT, *supra* note 14, 3(1), 3(2), 5(1), 5(2), 6(1), 9(1); *see also* Smith, *supra* note 53, at 120 ("The chief feature of this expedited access [provided by CLOUD Act Agreements] is the elimination of the responding government's role in approving the requesting government's order"); Kenneth Propp, *Introductory Note to 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*, 60 INT'L LEGAL MATERIALS 168, 168 (2021) (arguing that, by removing the role a requested state has in reviewing incoming requests, "[t]he CLOUD Act fundamentally changed the MLAT paradigm."); Marcin Rojszczak, *CLOUD Act Agreements from an EU Perspective*, 38 COMPUT. L & SEC. REV. 1, 2 (2020) ("[T]he leading role is played by the norms of national law").

117. US WHITE PAPER, *supra* note 111, at 6.

118. UK EXPLANATORY MEMORANDUM, *supra* note 77, ¶ 7; US WHITE PAPER, *supra* note 111, at 4–6; *see* Marco Stefan & Gloria González Fuster, *Cross-border Access to Electronic Data through Judicial Cooperation in Criminal Matters* 18 (CEPS Paper in Liberty and Security in Europe, Paper No. 2018-07, Nov. 2018, updated May 2019), https://www.ceps.eu/wp-content/uploads/2018/12/MSGGF_JudicialCooperationInCriminalMatters-2.pdf ("These

CLOUD Act agreements claim to protect digital privacy rights through several overarching *ex ante* mechanisms.[119] The US Attorney-General must certify to Congress that a country with which the US proposes to execute a CLOUD Act agreement provides sufficient rights protection,[120] although no statutory mechanism allows this certification to be challenged.[121] Signatories also agree to abide by their own digital privacy laws.[122] Additionally, CLOUD Act agreements require their parties to engage in periodic reviews of their compliance and data handling under it.[123]

There are two main routes through which digital privacy and other rights are said to be protected in practice.[124] One is targeting and minimization procedures—each state can use CLOUD Act agreements to target their own nationals or TCPs but normally not nationals of the other state.[125] Another protection is provided by service providers, who can object if they believe a request is improper under CLOUD Act agreement.[126] The provider's own state may eventually resolve such requests.[127] Other

---

requests would be compulsory upon the companies *based on the law of the issuing country*.") (emphasis in original).

119. *See* CLOUD Act § 105(a) (codified at 18 U.S.C. § 2523(b) (2018)) (listing requirements for obtaining a CLOUD Act agreement); Abraha, *supra* note 103, at 341–44; Daskal, *Law Enforcement Access*, *supra* note 40, at 494–96.

120. CLOUD Act § 105(a) (codified at 18 U.S.C. § 2523(b) (2018)); *see also* Clarifying Lawful Overseas Use of Data Act, Attorney General Certification and Determination, 85 Fed. Reg. 12578-01 (Mar. 3, 2020) (the US–UK Agreement certification).

121. *See e.g.,* CLOUD Act § 105(c) (codified at 18 U.S.C. § 2523I (2018)). Constitutional challenges may be possible. *See, e.g.*, Gutierrez de Martinez v. Lamagno, 515 U.S. 417, 424–25 (1995).

122. *See* US–UK AGREEMENT, *supra* note 4, at pmbl., arts. 2(1) 3(3), 8(1), 9, 10(10); US–AU AGREEMENT, *supra* note 14, at pmbl., arts. 2, 3(3), 3(4), 9(1).

123. *See* US–UK AGREEMENT, *supra* note 4, at art 12(1); *see also* The Functions of the Investigatory Powers Commissioner (Oversight of the Data Access Agreement between the United Kingdom and the United States of America and of functions exercisable under the Crime (Overseas Production Orders) Act 2019) Regulations 2020, SI 2020/1009 (UK).

124. *See infra* text accompanying notes 125–128.

125. *See* US–UK AGREEMENT, *supra* note 4, at arts. 1(12), 4, 7; US–AU AGREEMENT, *supra* note 14, at arts. 1(2), 1(13), 1(17), 4, 7; *see also* Abraha, *supra* note 103, at 336–338, 344–345 (elaborating on rationales for, and ambiguities arising from, these procedures).

126. *See* US–UK AGREEMENT, *supra* note 4, at arts. 5(11)–(12); US–AU AGREEMENT, *supra* note 14, at arts. 5(11)–(12).

127. *See* US–UK AGREEMENT, *supra* note 4, at arts. 5(11)–(12).

than this, CLOUD Act agreements presumes that a service provider's own state will have no involvement in, or even knowledge of, requests.[128] Where TCPs are targeted, a default obligation to notify a TCP's own state also applies.[129]

B. Assessing CLOUD Act Agreements against Digital Privacy Rights

1. The Fourth Amendment and Article 8

It is beyond the scope of this article to address the global recognition of digital privacy rights,[130] or normative arguments in favor.[131] Nonetheless, such rights clearly apply in the US and UK in the law enforcement context. The US Supreme Court recognized that the Fourth Amendment—protecting against "unreasonable searches and seizures" by public authorities—applied to protect digital privacy rights from improper government conduct in *Riley v. California*.[132] A similar judgment was given under Scottish law by Lord Ballantyne in June 2019, and included references to Article 8—which is even broader, providing a "right

128. This has been repeatedly noted in respect of orders from foreign CLOUD Act agreement states to US service providers. *See, e.g.*, Abraha, *supra* note 103, at 344, 350–351, 353 ("[T]here is no mechanism for the US government to ensure that each request issued by the qualifying legal government [party to a CLOUD Act agreement] meets the requirement[s] stipulated in the CLOUD Act."); Andrew Smith, *Overseas Production Orders: Getting Up to Speed*, 169 NEW L.J., 9, 9 (2019) ("The US authorities … have no power to review the [UK] judge's decision to grant the [overseas production order]."); *see also, e.g.*, Frederick T, Davis & Anna R. Gressel, *Storm Clouds or Silver Linings? The Impact of the U.S. CLOUD Act*, 45 LITIGATION, 1, 4 (2018) ("[T]he [CLOUD] Act provides no procedure for a recipient of an order from [non-US law enforcement] to contest that order in a U.S. court."). Given the reciprocity of CLOUD Act agreements, the same applies to CLOUD Act agreement requests from the US to foreign service providers. *See* sources cited *supra* note 112.

129. US–UK AGREEMENT, *supra* note 4, at art. 5(10); US–AU AGREEMENT, *supra* note 14, at art. 5(12).

130. *See supra* text accompanying note 37.

131. *See generally* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV L. REV. 193 (1890); *The Right to Privacy in the Digital Age*, *supra* note 11; ANDERSON, *supra* note 41, ¶¶ 2.8–2.13; Brunner, *supra* note 40.

132. Riley v. California, 573 U.S. 373, 393–401 (2014). The court has recently extended Fourth Amendment protections over other technological developments. *E.*g. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (cell phone tower location information); United States v. Jones, 565 U.S. 400, 404 (2012) (GPS tracking); Kyllo v. United States, 533 U.S. 27, 38-40 (2001) (thermal imaging).

to respect for … private and family life, … home and … correspondence."[133] Overall, direct UK recognition is less full-throated than in the US.[134] There is, however, ample ECtHR jurisprudence applying Article 8 in the digital sphere,[135] which must ordinarily be followed by UK courts.[136]

The direct impact of Fourth Amendment and Article 8 on law enforcement requests under CLOUD Act agreements is the focus of this article's comparative analysis for two reasons. First, they are commonly perceived to be the key constitutional mechanisms protecting privacy during law enforcement searches in these jurisdictions.[137] Additionally, while far from identical,[138] they share broad similarities,[139] enabling a rich comparative approach. This analysis may inform Council of Europe countries

133. BC v. Chief Constable of the Police Serv. of Scot. [2019] CSOH 48 [101]–[151], (2019) SLT 875, *aff'd on other grounds*, [2020] CSIH 61, (2021) SC 265 (Scot.).

134. R (T) v. Sec'y of State for the Home Dep't [2014] UKSC 35 [88], [2015] 1 AC 49 (appeal taken from Eng.); *see* Kirsty Hughes, *A Common Law Constitutional Right to Privacy – Waiting for Godot?*, *in* COMMON LAW CONSTITUTIONAL RIGHTS 91, 94 (Mark Elliott & Kirsty Hughes eds,. 2020).

135. Evangelia Psychogiopoulou, *The European Court of Human Rights, Privacy and Data Protection in the Digital Era*, *in* COURTS, PRIVACY AND DATA PROTECTION IN THE DIGITAL ENVIRONMENT 32 (Maja Brkan & Evangelia Psychogiopoulou eds., 2017); *e.g.*, Roman Zakharov v. Russia [GC], 2015-VIII Eur. Ct. H.R. 205 ¶¶ 227–305; Szabó & Vissy v. Hungary, App. No. 37138/14, ¶ 53 (Jan. 12, 2016), https://hudoc.echr.coe.int/fre?i=001-160020.

136. *See* HRA, § 2(1); R (Ullah) v. Special Adjudicator [2004] UKHL 26 [20], [2004] 2 AC 323 (appeal taken from Eng.); *see also* R (Hallam) v. Sec'y of State for Justice [2019] UKSC 2 [87]–[91] (Lord Wilson, J.S.C.), [125] (Lord Hughes), [2020] AC 279 (appeal taken from Eng.).

137. OFF. OF LEGAL EDUC., *supra* note 36, ix (referring to "the Fourth Amendment" as one of "two primary sources" of "[t]he law governing electronic evidence in criminal investigations"); LAW COMMISSION, *supra* note 37, ¶¶ 14.88, 14.19 ("Powers of search and seizure predominantly engage article 8.").

138. STEFAN SOTTIAUX, TERRORISM AND THE LIMITATION OF RIGHTS: THE ECHR AND THE US CONSTITUTION 273 (2008); Kirsty Hughes & Neil M. Richards, *The Atlantic Divide on Privacy and Free Speech*, *in* COMPARATIVE DEFAMATION AND PRIVACY LAW 164, 165 (Andrew T. Kenyon ed., 2016). *See generally* Bignami & Resta, *supra* note 89; Peter Swire & DeBrae Kennedy-Mayo, *How Both the EU and the U.S. Are "Stricter" Than Each Other for the Privacy of Government Requests for Information*, 66 EMORY L. J. 617 (2017).

139. SOTTIAUX, *supra* note 138, at 268; Hughes & Richards, *supra* note 138, at 166.

subject to the ECHR but not in the EU, such as Switzerland.[140] It may also guide jurisdictions with protections similar to the US here, such as New Zealand.[141]

2. Other Issues and Rights Engaged

Other potential Fourth Amendment and Article 8 concerns, while outside the scope of this article, deserves future consideration. The US and UK may be complicit for any breaches of privacy effected by the other pursuant to CLOUD Act agreements, on the basis they have granted express permission to the other state to act within their territory.[142] Whether service providers' should be treated as state actors or public authorities—thus subject to the Fourth Amendment and Article 8—when responding to CLOUD Act requests is debatable.[143] It is also settled ECHR law that, "[w]hile the essential object of the [ECHR] is to protect individuals against arbitrary interference by public authorities, it may also impose on the State certain *positive obligations* to

---

140. *See, e.g.*, Tarakhel v. Switzerland [GC], 2014-VI Eur. Ct. H.R. 195, ¶ 88 (noting that, although "Switzerland is not a Member State of the European Union," its "responsibility" under the ECHR was "not disputed").

141. New Zealand law provides protections similar to the Fourth Amendment that have been extended to the digital arena. *See* New Zealand Bill of Rights Act 1990, s 21 (N.Z.); *Dotcom v. Att'y-Gen.* [2014] NZSC 199 [191], [2015] 1 NZLR 745 (N.Z.). Evidence obtained in breach of these protections may face exclusion during criminal proceedings. *See* Evidence Act 2006, s 30 (N.Z.). However, while New Zealand has a comprehensive data protection statute, Privacy Act 2020 (N.Z.), even "serious" breaches of that legislation alone are not sufficient to trigger exclusion. *R v. Alsford* [2017] NZSC 42 [39]–[40], [47], [73], [2017] 1 NZLR 710 (N.Z.). For further analysis discussing a potential 'US–NZ' CLOUD Act Agreement, see generally Tim Cochrane, *Law Enforcement Cross-Border Data Sharing: A CLOUD Act Agreement for Aotearoa New Zealand?,* [2021] N.Z. L. REV. 403.

142. El-Masri v. The Former Yugoslav Republic of Macedonia [GC], 2012-VI Eur. Ct. H.R. 263 ¶ 206; Marko Milanovic, *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age,* 56 HARV. INT'L L.J. 81, 123 (2015); Patricia L. Bellia, *Chasing Bits Across Borders*, U. CHI. LEGAL F. 35, 98 (2001) (citing Skinner v. Ry Lab. Execs. Ass'n., 489 U.S. 602, 614–15 (1989)).

143. Allison M. Holmes, *Private Actor or Public Authority? How the Status of Communications Service Providers Affects Human Rights*, 22 COMMS. L. 1, 21 (2017); *e.g.*, *R v. Cox* (2004) 21 CRNZ 1 (CA) at [37]–[38] (N.Z.); *see* Stanislaw Tosza, *Mutual Recognition by Private Actors in Criminal Justice? Service Providers as Gatekeepers of Data and Human Rights Obligations*, COMMON MKT. L. REV. (forthcoming 2022) (manuscript at 20), https://ssrn.com/abstract_id=3517878; Bellia, *supra* note 142, at 90–95. *But see, e.g.*, Richardson v. Facebook [2015] EWHC 3154 [60]–[63] (QB) (Eng.).

ensure effective respect for the rights protected by Article 8,"[144] such as to adopt a legal framework to protect against privacy breaches by third parties.[145] Whether implementing CLOUD Act agreement frameworks are sufficient from that perspective should be separately considered.

Other constitutional and human rights may also be engaged. These include due process or fair trial rights,[146] the evolving prohibition against the death penalty,[147] and data protection rights. The long-term application of EU data protection law in the UK is uncertain following Brexit,[148] and such rights receive limited protection under US federal law.[149] Nonetheless, the compatibility of direct access mechanisms with data protection law is a significant developing issue, given legislation like the General Data Protection Regulation (GDPR),[150] as well as recent case law from

144. Bărbulescu v. Romania [GC], App. No. 61496/08, ¶ 108 (Sept. 5, 2017), https://hudoc.echr.coe.int/eng?i=001-177082. *See generally* DIMITRIS XENOS, THE POSITIVE OBLIGATIONS OF THE STATE UNDER THE EUROPEAN CONVENTION OF HUMAN RIGHTS (2012).

145. *E.g.*, *Bărbulescu*, App. No. 61496/08, ¶ 119–20. I am grateful to Dr. Kristy Hughes for raising this point.

146. *See* U.S. CONST. amends. V, XIV, §1; ECHR, *supra* note 9, at art. 6. For due process concerns, see Rutherford*, supra* note 13, at 1190; SHELLI GIMELSTEIN, DATA CATALYST, STORM ON THE HORIZON: HOW THE U.S. CLOUD ACT MAY INTERACT WITH FOREIGN ACCESS TO EVIDENCE AND DATA LOCALIZATION LAWS 6–7 (2019).

147. *See* Tim Cochrane, *The Impact of the CLOUD Act Regime on the UK's Death Penalty Assurances Policy*, U.K. CONSTITUTIONAL 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/.

148. Irena Ilic, *Post-Brexit Limitations to Government Surveillance: Does the UK get a Free Hand?*, 25 COMMS. L. 31, 31–32 (2020). *See generally* Data Protection Act 2018, c.12, ch. 2 (U.K.) (incorporating, at U.K. law, Commission and Parliament Regulation 2016/679, 2016 O.J. (L 119) 1 (repealing Directive 95/46/EC) (General Data Protection Regulation) [hereinafter GDPR]); *see also* Data Protection Act 2018, c.12, ch. 3 (incorporating the GDPR's law enforcement equivalent).

149. SOTTIAUX, *supra* note 138, at 265; Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771, 811 (2019).

150. GDPR, *supra* note 148. The GDPR will likely function as a "blocking statute" in this context. *See* 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, 170–77 (2020); *e.g.*, Rutherford, *supra* note 13, at 1199–200.

the UK and the Court of Justice of the European Union (CJEU).[151]

C. 'Business as Usual' or 'A Race to the Bottom'?

1. Overall Reception

The attitude taken to CLOUD Act agreements largely divides on predictable lines.[152] International interest has been expressed by other 'Five Eyes' countries and close US partners.[153] Australia signed a CLOUD Act Agreement with the US in December 2021,[154] and support has also been expressed in Canada and New Zealand.[155] Standing in some contrast is the EU. The Commission has raised doubts as to whether the US–UK Agreement complies with EU law,[156] while EU privacy authorities have

---

151. Recent GDPR caselaw emphasizes the importance of complying with data protection requirements in cross-border contexts. *E.g.*, Case C-311/18, Data Prot. Comm'r. v. Facebook Ir. Ltd., ECLI:EU:C:2020:559, ¶¶ 198-99 (July 16, 2020); Elgizouli v. Sec'y of State for the Home Dep't [2020] UKSC 10, [2021] AC 937 (appeal taken from Eng.); *see* Siofra O'Leary, *Balancing Rights in the Digital Age*, IRISH JURIST 59, 81 (2018).

152. *See* MULLIGAN, *supra* note 88, at 21–22.

153. *See* Propp, *supra* note 116, at 169; Theodore Christakis, *E-EVIDENCE: The Way Forward (Summary of the Workshop Held in Brussels on 25 September 2019)* EUR. L. BLOG (Nov. 6, 2019), https://europeanlawblog.eu/2019/11/06/e-evidence-the-way-forward-summary-of-the-workshop-held-in-brussels-on-25-september-2019/; 164 CONG. REC. S1923 (daily ed. March 22, 2018) (statement of Sen. Hatch) (suggesting the US–UK Agreement may "serve as a model for future agreements between the United States and other countries"); 792 Parl Deb HL (5th ser.) (2018) col. 921 ("[W]e are looking . . . to establish a reciprocal arrangement with the USA and presumably with the other Five Eyes countries in due course, in addition to other countries."). 'Five Eyes,' also known as '5VEY' and formally referred to as 'UKUSA', "is widely regarded as the world's most significant intelligence alliance." *See* J Vitor Tossini, *The Five Eyes – The Intelligence Alliance of the Anglosphere,* U.K. DEF. J. (April 14, 2020), https://ukdefencejournal.org.uk/the-five-eyes-the-intelligence-alliance-of-the-anglosphere/.

154. *See* sources cited *supra* note 14.

155. *See* Public Safety Canada, *CLOUD Act*, Briefing Book for the Minister of Public Safety Canada (Nov. 20, 2019), https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/trnstn-bndrs/20191120/034/index-en.aspx; Cochrane, *supra* note 141, at 402, 402 n.5.

156. *See, e.g.*, UK Adequacy Decision, *supra* note 7, (153)–(156); *Answer Given by Mr Reynders on Behalf of the European Commission*, *Question Reference:* E-003136/2019(ASW), EUR. PARLIAMENT (Jan. 10, 2020), https://www.europarl.europa.eu/doceo/document/E-9-2019-003136-ASW_EN.html.

expressed concerns.[157] US–EU negotiations to resolve international law enforcement data sharing are ongoing.[158] Global service providers, who have long sought a solution to the conflict of laws problem they face,[159] are broadly supportive,[160] while human rights NGOs appear uniformly critical.[161]

Initial academic analysis of CLOUD Act agreements came from the US. The main commentators there, Swire, Daskal, and Woods, were the early advocates of such a direct access model for the US, and are thus unsurprisingly strongly supportive.[162]

---

157. Letter from Andrea Jelinek, Chair of the European Data Protection Board, to Members of the European Parliament 1 (June 15, 2020), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out_2020-0054-uk-usagreement.pdf.

158. Press Release, U.S. Dep't of Justice, *Joint US–EU Statement on Electronic Evidence Sharing Negotiations* (Sept. 26, 2019), https://www.justice.gov/opa/pr/joint-us-eu-statement-electronic-evidence-sharing-negotiations.

159. ANDERSON, *supra* note 41, ¶¶ 11.8–11.12, 11.18, 11.24; Woods, *supra* note 42, at 673–74.

160. Letter from Apple, Facebook, Google, Microsoft & Oath, to Sens. Orrin Hatch, Lindsey Graham, Christopher Coons & Sheldon Whitehouse (Feb. 6, 2018), https://blogs.microsoft.com/wp-content/uploads/sites/149/2018/02/Tech-Companies-Letter-of-Support-for-Senate-CLOUD-Act-020618.pdf [hereinafter Service Providers Letter]; *e.g.*, Brad Smith, *A Call for Principle-Based International Agreements to Govern Law Enforcement Access to Data*, MICROSOFT: MICROSOFT ON THE ISSUES BLOG (Sept. 11, 2018), https://blogs.microsoft.com/on-the-issues/2018/09/11/a-call-for-principle-based-international-agreements-to-govern-law-enforcement-access-to-data/.

161. Letter from Human Rights Watch, Access Now, Demand Progress, Electronic Frontier Foundation, Fight for the Future, Freedom of the Press Foundation & Government Accountability Project, to Richard W. Downing, Acting Deputy Assistant Att'y Gen. (Nov. 26, 2018), https://www.hrw.org/news/2018/11/26/letter-us-justice-department-concluding-white-house-should-not-let-uk-demand# [hereinafter HRW Letter].

162. *E.g.*, Andrew Keane Woods & Peter Swire, *The CLOUD Act: A Welcome Legislative Fix for Cross-Border Data Problems*, LAWFARE (Feb. 6, 2018, 5:49 PM), https://www.lawfareblog.com/cloud-act-welcome-legislative-fix-cross-border-data-problems; Jennifer Daskal & Andrew Keane Woods, *Congress Should Embrace the DOJ's Cross-Border Data Fix*, LAWFARE (Aug. 1, 2016, 8:52 AM), https://www.lawfareblog.com/congress-should-embrace-dojs-cross-border-data-fix-0. U.S. authors predominantly support it. *E.g.*, Schwartz, *supra* note 44, at 1748–49 (concluding "[t]he decentralized approach of the CLOUD Act [regime] is promising," with "important elements . . . that protect privacy," but cautioning "much, however, . . . is open concerning the ultimate impact"); *cf.* Secil Bilgic, Note, *Something Old, Something New, and Something Moot: The Privacy Crisis Under the CLOUD Act*, 32 HARV. J. L. & TECH. 321, 353 (2018) ("[The CLOUD Act agreement model] not only risks the privacy of U.S. citizens

It would not, however, be accurate to describe them as uncritical backers. Daskal's position, describing CLOUD Act agreements as "not perfect" but "nonetheless a step forward," is representative.[163] More recently, extensive scholarship has emerged elsewhere, primarily from Europe.[164] Much of this discusses CLOUD Act agreements in the context of the related EU direct access proposals.[165] In stark contrast with the dominant US perspective, however, European views of CLOUD Act agreements to date are largely negative, based on rights concerns, as addressed below.

2. Perceived Impact on Digital Privacy Rights

On the US side of the Atlantic, CLOUD Act agreements are largely seen as 'business as usual' or even positive for digital

---

by allowing unlimited access to qualifying foreign governments, but also threatens the privacy of foreign citizens."); *see also* Smith, *supra* note 53, at 120 (referring to the potential extraterritorial scope of surveillance powers under CLOUD Act agreements as "unsettling").

163. Daskal, *Borders and Bits*, *supra* note 46, at 229; *e.g.*, Swire & Kennedy-Mayo, *supra* note 138, at 625 ("We are cautiously supportive."); Zarine Kharazian, *The CLOUD Act: Arguments For and Against*, 34 INT'L ENF'T L. REP. 159, 161 (2018) ("The CLOUD Act is certainly not perfect. . . . On balance, however, [it] is a welcome, albeit overdue, step in the right direction.").

164. *E.g.*, JULIA HÖRNLE, INTERNET JURISDICTION: LAW AND PRACTICE 211–15 (2021); Halefom 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 (2021) [hereinafter Abraha, *Mapping Policy*]; Abraha, *supra* note 103; Abraha, *supra* note 64; de Busser, *Digital Unfitness*, *supra* note 65; de Busser, *EU-US*, *supra* note 36; Galvagna, *supra* note 64, at 66–67; Eleni Kyriakides, *The CLOUD Act, E-Evidence, and Individual Rights*, 5. EUR. DATA. PROT. 99 (2019); Rojszczak, *supra* note 116; Shurson, *supra* note 150; Siry, *supra* note 64; SERGIO CARRERA, MARCO STEFAN & VALSAMIS MITSILEGAS, REPORT OF A CEPS AND QMUL TASK FORCE, CROSS-BORDER DATA ACCESS IN CRIMINAL PROCEEDINGS AND THE FUTURE OF DIGITAL JUSTICE: NAVIGATING THE CURRENT LEGAL FRAMEWORK, AND EXPLORING WAYS FORWARD WITHIN THE EU AND ACROSS THE ATLANTIC (2020), https://www.ceps.eu/download/publication/?id=30689&pdf=TFR-Cross-Border-Data-Access.pdf; Stefan & Fuster, *supra* note 118; 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/ [hereinafter Christakis, *21*].

165. *See*, *e.g.*, Stefan & Fuster, *supra* note 118, at iv; de Busser, *Digital Unfitness*, *supra* note 65, at 163; de Busser, *EU-US*, *supra* note 36, at 1260–66; *see also* Siry, *supra* note 64, at 237–45.

privacy rights. US analysis concentrates on the impact of CLOUD Act agreements on Fourth Amendment rights,[166] and in particular whether US persons' Fourth Amendment rights may be breached through incoming CLOUD Act agreements requests from foreign states to US providers.[167] Although counterparties to CLOUD Act agreements are barred from directly targeting US persons,[168] there is broad acceptance that "incidental collection" of US persons' data through foreign state requests is likely, if not "almost certain,"[169] and an equally common view that UK law offers less extensive protections than US law, at least in some areas, such as when intercepting data.[170] Having considered this issue, Swire and Justin Hemmings express "serious doubts about whether the scale and nature of the incidental collection would violate the Fourth Amendment."[171]

US discussion of the impact of CLOUD Act agreements on *non*-US persons' Fourth Amendment rights typically begins (and

---

166. SWIRE & HEMMINGS, OVERCOMING, *supra* note 13, at 6–14; Schwartz, *supra* note 44, at 1708–14; *see also* Daskal, *Un-Territoriality*, *supra* note 1 (centering an analysis of law enforcement extraterritorial data gathering generally within the Fourth Amendment); Orin S. Kerr, *The Fourth Amendment and the Global Internet* 67 STAN. L. REV. 285, 288–89 (2015) (similar).

167. Bilgic, *supra* note 162, at 323; *see, e.g.*, SWIRE & HEMMINGS, OVERCOMING, *supra* note 13, at 6–14 (citing HRW Letter, *supra* note 161); Eddie B. Kim, Note, *U.S.-UK Executive Agreement: Case Study of Incidental Collection of Data Under the CLOUD Act*, 15 WASH. J. L., TECH. & ARTS 247, 253 (2020).

168. *See* US–UK AGREEMENT, *supra* note 4, at arts. 1(12), 4(3), 7; US–AU Agreement, *supra* note 14, at arts. 1(2), 1(13), 1(17), 4, 7.

169. Schwartz, *supra* note 44, at 1751 (referring to "incidental collection" as "likely"); Daskal, *Privacy and Security*, *supra* note 36, at 1048 ("Foreign government access is likely, in fact almost certain, to yield broad incidental collection."); *see* HÖRNLE, *supra* note 164, at 215 ("The targeting [restriction], however, [requires] only a good faith effort on both sides, as it may not be clear in a case at hand where the target is or who runs an account."); *see also* SWIRE & HEMMINGS, OVERCOMING, *supra* note 13, at 13 (suggesting "the scale" of incidental collection will likely be low).

170. *E.g.*, Swire & Kennedy-Mayo, *supra* note 138, at 644–46; *see* Schwartz, *supra* note 44, at 1750–51.

171. SWIRE & HEMMINGS, OVERCOMING, *supra* note 13, at 14. *Contra* Kim, *supra* note 167, at 251 ("[T]he threat to data privacy of US citizens via incidental collection under the CLOUD Act is not only possible, but probable."); *see also* Swire & Kennedy-Mayo, *supra* note 138, at 664 and 664 n. 230 ("[W]e have reservations about . . . whether a foreign government can constitutionally intercept real-time communications in the United States without US judicial oversight.").

largely ends) by referencing the Supreme Court judgment *United States v. Verdugo-Urquidez*.[172] This is commonly applied as authority that Fourth Amendment protections do not generally extend to TCPs (or UK nationals); they only obtain Fourth Amendment rights after they have voluntarily entered the US and developed "substantial connections" there.[173] In the context of analyzing CLOUD Act agreements, US analysis generally assumes, if not avowedly defends, this orthodox *Verdugo-Urquidez* approach.[174] Seen that way, CLOUD Act agreements will apparently not materially undermine TCPs' digital privacy rights because TCPs typically have no recognized rights to undermine. Separately, US analysis positively argues that CLOUD Act agreements will benefit TCPs' digital privacy rights, because foreign states will have a "significant motivation . . . to increase protections for privacy and civil liberties" to meet the US' minimum requirements for joining.[175] Indeed, Daskal suggests that

172. United States v. Verdugo-Urquidez, 494 U.S. 259 (1990); *see* SWIRE & HEMMINGS, OVERCOMING, *supra* note 13, at 7–8; Schwartz, *supra* note 44, at 1709–14; Bilgic, *supra* note 162, at 349 n.171; Swire & Hemmings, *Visa Waiver*, *supra* note 82, at 737; *see also* Kerr, *supra* note 166, at 301 (accepting "the basic principles of existing doctrine" that "[o]nly persons with sufficient contacts with the United States have Fourth Amendment rights"). *Verdugo-Urquidez* concerned whether a Mexican criminal defendant with no previous US ties had standing to allege that a warrantless search of their property in Mexico while they were detained in the United States should be excluded under the Fourth Amendment. *Verdugo-Urquidez*, 494 U.S. at 462–63. The Court, in a plurality opinion given by Rehnquist, C.J., ruled that the defendant lacked such standing on the basis that non-resident non-nationals only "receive constitutional protections when they have come within the territory of the United States and developed substantial connections with this country." *Id.* at 271.

173. Jennifer Daskal & Stephen I. Vladeck, *"Incidental" Foreign Intelligence Surveillance and the Fourth Amendment*, *in* THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW 101, 105 (David Gray & Stephen E. Henderson eds., 2017); *e.g.,* United States v. Muhtorov, 20 F.4th 558, 593–594 (10th Cir. 2021); United States v. Emmanuel, 565 F.3d 1324, 1331 (11th Cir. 2009) (citing *Verdugo-Urquidez*, 494 U.S. at 275).

174. *E.g.,* Peter Swire, Jesse Woo & Deven R. Desai, *The Important, Justifiable, and Constrained Role of Nationality in Foreign Intelligence Surveillance* 5 (Hoover Working Grp. On Nat'l Sec., Tech. & L., Aegis Series Paper No. 1901, 2019), https://www.hoover.org/sites/default/files/research/docs/swire-woo-desai_the-important-justifiable-constrained-role-of-nationality-in-foreign-intelligence-surveillance1.pdf.

175. US WHITE PAPER, *supra* note 111, at 13; *e.g.*, Daskal & Woods, *supra* note 162 (arguing this may cause "a significant enhancement of privacy protections globally"); Jennifer Daskal & Peter Swire, *Privacy and Civil Liberties Under the CLOUD Act: A Response*, LAWFARE (Mar. 21, 2018, 7:00 AM),

privacy-enhancing amendments to UK surveillance law were made partly for that very reason.[176]

A starkly different view is taken on the other side of the Atlantic (and elsewhere), where CLOUD Act agreements are viewed as potentially presaging a 'race to the bottom' for rights.[177] Most focus to date has been on EU data protection law,[178] although academics have also expressed disquiet over the impact on rights protected by the ECHR, including Article 8.[179] Repeated

---

https://www.lawfareblog.com/privacy-and-civil-liberties-under-cloud-act-response (similar). *But see* Andrew Keane Woods, *Litigating Data Sovereignty*, 28 YALE L. J. 328, 400–01 (2018) (accepting that a CLOUD Act "club of insider countries could ideally create a race to the top" for privacy protections, but warning that "clubs lead to anticlubs – and China is actively pursuing just such a club."). Julia Hörnle, writing from the UK, additionally warns that "it may also lead to a lowering of safeguards, as countries with higher safeguards . . . might have to tolerate US law enforcement carrying out investigative measures without recourse to national, non-US law." HÖRNLE, *supra* note 164, at 213.

176. Daskal, *Borders and Bits*, *supra* note 46, at 204–05; *see* Sujit Raman, Assistant Deputy Att'y Gen., US Dep't of Justice, 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 ("[T]he United Kingdom undertook changes to its own laws in order to assure that it could comply with the CLOUD Act's requirements.").

177. *E.g.*, HÖRNLE, *supra* note 164, at 214 (expressing concerns for individuals' rights under CLOUD Act agreements, arguing that these do "not guarantee . . . mutually agreed privacy standards nor accessible judicial review"); de Busser, *EU-US*, *supra* note 36, at 1266–67 (referring critically to new direct access regimes as "not . . . beneficial . . . when guarantees protecting states' sovereignty and individuals' rights" are left behind); Siry, *supra* note 64, at 229 ("[The CLOUD Act agreement model's] potential is to disrupt the rights protection regime of European citizens"); de Busser, *Digital Unfitness*, *supra* note 65, at 178–79 ("[The effect [from CLOUD Act agreements] of circumventing the safeguards built into the MLA cooperative mechanism is alarming."); *see also* Stefan & Fuster, *supra* note 118, at v (expressing "serious doubts" about whether EU member states can or should enter into CLOUD Act regime agreements). *But see* Eneli Laurits, *Regulating the Unregulatable: An Estonian Perspective on the CLOUD Act and the E-Evidence Proposal*, 29 JURIDICA INT'L 62, 64 (2020) (expressing more positive views).

178. *See* Rojszczak, *supra* note 116, at 9–12; Shurson, *supra* note 150, at 176; Abraha, *supra* note 64, at 209–11; Stefan & Fuster, *supra* note 118, at 20; CARRERA, STEFAN & MITSILEGAS, *supra* note 164, at 35.

179. *E.g.*, Siry, *supra* note 64, at 229 (arguing CLOUD Act agreements may circumvent "fundamental rights protections guaranteed by the [ECHR]"); *see* Stefan & Fuster, *supra* note 118, at 12–13 (discussing Article 8 requirements applicable to cross-border law enforcement requests).

concerns have been raised about the removal of MLA's supposed safeguards and the adequacy of replacements provided by CLOUD Act agreements.[180] For example, Els de Busser considers that "the effect of circumventing the safeguards built into the MLA cooperative mechanism is alarming."[181] She explains that the country where data is located, which previously would have executed a US MLA request for this data under its own law, now "has no voice in the matter."[182] Julia Hörnle argues that the CLOUD Act model "does not satisfy" individuals' privacy needs because it "purely relies on the safeguards in the issuing state, which may not cover the privacy interests" of a target.[183] The appropriateness of making service providers primarily responsible for "safeguarding the interests of the states and individuals involved" also comes in for significant criticism.[184]

II. COMPARING DIGITAL PRIVACY RIGHTS UNDER MLA WITH CLOUD ACT AGREEMENTS

Part II evaluates the impact of CLOUD Act agreements on digital privacy rights from the perspective of the three classes of potentially affected persons: US persons, UK persons, and TCPs, each of whom is assumed to be physically based in their own territory. It compares the rights they have under MLA with their equivalent position under the US–UK Agreement, addressing both *ex ante* and *ex post* protections at three key stages.[185] It assumes that US persons' data is most likely to be sought from the US, and UK persons' data from the UK, although it also considers the reciprocal scenario for each. It shows that the contrasting literature views are each partly right and partly wrong; while

180. *See infra* text accompanying notes 181–183.

181. de Busser, *Digital Unfitness*, *supra* note 65, at 178; *see* Siry, *supra* note 64, at 250 (referring to the removal of MLA's "built-in system of double control" as "[p]ossibly the most troubling aspect of" direct access mechanisms).

182. de Busser, *Digital Unfitness*, *supra* note 65, at 178; *see* HÖRNLE, *supra* note 164, at 211 (arguing CLOUD Act agreements rely on a "notion of 'general trust,'" which "creates a dangerous precedent as compliance with fundamental rights needs to be checked on a case-by-case basis").

183. HÖRNLE, *supra* note 164, at 213; *see* Abraha, *Mapping Policy*, *supra* note 164, at 149 (expressing concerns that the reach of CLOUD Act agreements to TCPs "could generate new conflicts of laws and exacerbate existing ones").

184. de Busser, *EU-US*, *supra* note 36, at 1266–67; *see* HÖRNLE, *supra* note 164, at 215; Abraha, *supra* note 103, at 148–49; Stefan & Fuster, *supra* note 118, at 50.

185. ZEEGERS, *supra* note 70, at 137; *see* BOISTER, *supra* note 2, at 311.

rights are largely improved for US and UK persons, they are significantly diminished for TCPs.[186]

A. MLA Fails to Protect US Persons' Digital Privacy Rights

US–UK MLA offers US persons—indeed, all persons—significantly fewer protections for digital privacy rights than when these states gather evidence domestically.[187] In principle, the US is required to act consistently with the Fourth Amendment in its dealings with US persons at all times,[188] but in practice this provides limited protections. The UK, in contrast, will not extend Article 8 protections to US persons during MLA.[189] MLA processes in each jurisdiction fail to uphold digital privacy rights, providing US persons with very limited protections during all three MLA stages.[190] Most notably, the key protection for US persons' digital privacy rights here—the *ex post* ability to seek to exclude evidence in criminal proceedings[191]—is almost always unavailable.

1. Initial US Steps

The US MLA process typically begins with US law enforcement contacting the Office of International Affairs (OIA) within the US Department of Justice.[192] OIA acts as the US' central

186. *See* discussion *infra* Sections II.B, II.D–II.E.

187. For domestic US protections, *see* WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT (6th ed. 2020); OFF. OF LEGAL EDUC., *supra* note 36. For the UK, *see* POLICE AND CRIMINAL EVIDENCE ACT (PACE) CODE B: REVISED CODE OF PRACTICE FOR SEARCHES OF PREMISES BY POLICE OFFICERS AND THE SEIZURE OF PROPERTY FOUND BY POLICE OFFICERS ON PERSONS OR PREMISES (2013), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/903811/pace-code-b-2013.pdf [hereinafter PACE CODE B]; MICHAEL ZANDER, ZANDER ON PACE: THE POLICE AND CRIMINAL EVIDENCE ACT 1984 § 2 (8th ed. 2018).

188. Weeks v. United States, 232 U.S. 383, 391–92 (1914); Elkins v. United States, 364 U.S. 206, 208–24 (1960); Berger v. New York, 388 U.S. 41, 49–64 (1967); *see* Boumediene v. Bush, 553 U.S. 723, 765 (2008).

189. *See infra* text accompanying notes 240–251.

190. *See infra* text accompanying notes 192–271.

191. United States v. Grubbs, 547 U.S. 90, 99 (2006). Civil remedies may be available. *E.g.*, Bivens v. Six Unknown Named Agents of Federal Bureau of Narcotics, 403 U.S. 388 (1971).

192. Thomas G. Snow, *The Investigation and Prosecution of White-Collar Crime: International Challenges and the Legal Tools Available to Address Them*, 11 WM. & MARY BILL RTS. J. 209, 227 (2002); *see* U.S. DEP'T OF JUSTICE,

authority responsible for drafting, approving, and transmitting MLA requests,[193] including requests for overseas electronic data.[194] The US may only request stored data; interceptions of live data (also known as wiretaps)[195] are unavailable from the UK.[196] OIA's involvement in, and initial screening of, requests provides some *ex ante* protection to US persons.[197]

It is, however, very difficult to challenge OIA's initial steps. Affected persons are very unlikely to know an MLA request has been made until after the process is complete.[198] Requests are confidential,[199] typically issued solely by OIA without court

---

JUSTICE MANUAL §§ 9–13.510, 9–13.514 (2020) [hereinafter JUSTICE MANUAL] (recommending early Office of International Affairs [OIA] contact).

193. Central or Competent Authority under Treaties and Executive Agreements on Mutual Assistance in Criminal Matters, 28 C.F.R. § 0.64–1 (2020); JUSTICE MANUAL, *supra* note 192, §§ 9–13.500 to 9–13–525; *see* T. Markus Funk, *The Key Tools of the Trade in Transnational Bribery Investigations and Prosecutions: Mutual Legal Assistance Treaties (MLATs) and Letters Rogatory*, *in* UNDERSTANDING THE GLOBAL FIGHT AGAINST CORRUPTION AND GRAFT 547, 550 (T. Markus Funk & Andrew S. Boutros eds., 2019); Snow, *supra* note 192, at 227–28.

194. JUSTICE MANUAL, *supra* note 192, §§ 9–13.514, 9–13.525.

195. *See* Wiretap Act, 18 U.S.C. 119 §§ 2510–2523 (2018).

196. U.K. HOME OFFICE, REQUESTS FOR MUTUAL LEGAL ASSISTANCE IN CRIMINAL MATTERS: GUIDELINES FOR AUTHORITIES OUTSIDE OF THE UNITED KINGDOM 30 (12th ed. 2015) [hereinafter UK MLA GUIDELINES]; IAN WALDEN, COMPUTER CRIMES AND DIGITAL INVESTIGATIONS § 5.60 (2d ed. 2016).

197. *See* Snow, *supra* note 192, at 227–28; *see also* sources cited *supra* note 188.

198. *See infra* text accompanying notes 199–200.

199. US–UK MLAT, *supra* note 61, at art. 7(1); *see International Enquiries*, CROWN PROSECUTION SERVICE [CPS] (July 1, 2019), https://www.cps.gov.uk/legal-guidance/international-enquiries (elaborating this and other legislation); *see supra* text accompanying notes 63–65 ("It is usual policy for central … authorities to neither confirm nor deny the existence of an MLA request."); Matos v. Reno, No. 96 CIV. 2974 (MBM), 1996 WL 467519, at *2 (S.D.N.Y. Aug. 16, 1996) ("Unless directed otherwise … OIA[] keeps confidential such requests for assistance."); R (Terra Servs.' Ltd.) v. National Crime Agency [2019] EWHC (Admin) 3165 [16]–[17], [2020] Lloyd's Rep. F.C. 29 (noting the confidentiality of US–UK MLA relations specifically); Bloomberg LP v. ZXC [2022] UKSC 5 [11]–[17], [148] (appeal taken from Eng.) (upholding the confidentiality of an MLA request from the UK to an unnamed country); Dongkuk Int'l, Inc. v. U.S. Dep't of Just., 204 F.Supp.3d 18, 22, 27–28 (D.D.C. 2016) (upholding the confidentiality of an MLA request to the United States under an MLAT materially similar to the US–UK MLAT).

input.[200] Even if an affected person had timely knowledge of a request, there are normally no meaningful grounds on which they could object. Arguments arising from the US–UK MLAT are barred.[201] A decision to issue an MLA request may theoretically be challenged on constitutional grounds, but no challenges appear to have been successful.[202] A wide discretion is afforded here to the US government.[203] It would, in any event, be difficult, if not impossible, to establish that an applicant has 'standing' under the Fourth Amendment at this stage, as discussed below.[204]

2. UK Execution of US Requests

Requests are typically transmitted to the UK Central Authority (UKCA) within the UK Home Office,[205] and dealt with under

---

200. Funk, *supra* note 193, at 548. *But see id.* at 561 (noting courts may become indirectly involved); *e.g.*, United States v. Wilson, 322 F.3d 353 (5th Cir. 2003).

201. US–UK MLAT, *supra* note 61, at art. 1(3); *In re* Request from the United Kingdom Pursuant to Treaty Between the Gov't. of the United States & the Gov't of the United Kingdom on Mut. Assistance in Criminal Matters in the Matter of Dolours Price, 685 F.3d 1, 11–13 (1st Cir. 2012); United States v. $734,578.82 in U.S. Currency, 286 F.3d 641, 659 (3d Cir. 2002); Gane & Mackarel, *supra* note 19, at 105–08.

202. *In re* Request from the United Kingdom Pursuant to the Treaty Between the Gov't. of the United States & the Gov't. of the United Kingdom on Mut. Assistance in Criminal Matters in the Matter of Dolours Price, 718 F.3d 13, 23 (1st Cir. 2013); *Dolours Price*, 685 F.3d at 15; *In re* Premises Located at 840 140th Ave. NE, Bellevue, Wash., 634 F.3d 557, 574 (9th Cir. 2011); RESTATEMENT (FOURTH) OF FOREIGN RELATIONS LAW § 429, Reps.' Notes at 6 (AM. BAR ASS'N 2018); *see* United States v. McLellan, 959 F.3d 442, 471–76 (1st Cir. 2020) ("The Constitution may protect individuals in the United States from subpoenas to comply with foreign MLAT requests."); *see also In re Ex parte* Petition of the Republic of Turkey for an Order Directing Discovery from Hamit Çiçek Pursuant to 28 U.S.C. § 1782, No. 2:19-CIV-20107-ES-SCM, 2020 WL 2539232, at *6 (D.N.J. May 18, 2020) (stating foreign MLA requests are "subject to judicial review and Constitutional guarantees"), *vacated*, Re: Republic of Turkey v. Cicek, No. 19-20107 (ES) (SCM), 2020 WL 8073613 (D.N.J. June 4, 2020); Palmat Int'l, Inc. v. Holder, No. 12-20229-CIV, 2013 WL 594695, at *3–*5 (S.D. Fla., Feb. 13, 2013) (agreeing that the constitutionality of MLAT actions can be challenged).

203. *In re* Premises, 634 F.3d at 572 (citing Zschernig v. Miller, 389 U.S. 429, 432 (1968)); *e.g.*, United States v. Bases, No. 18 CR 48, 2020 WL 5909072, at *4 (N.D. Ill. Oct. 6, 2020) (upholding merely "pretextual" MLATs).

204. *See infra* sources cited at note 284 and accompanying text.

205. *See* UK MLA GUIDELINES, *supra* note 196, at 4–5.

the UK's main MLA statute, the Crime (International Co-operation) Act 2003 (CICA).[206] Some *ex ante* protection may be provided by UKCA's role,[207] although UK courts have stressed that UKCA's initial review "should be simple."[208] UKCA will refer a compliant request to law enforcement, who will normally separately determine the appropriate method for obtaining the information requested.[209] To obtain communications content from a UK service provider, law enforcement typically seeks a 'production order,'[210] using a combination of CICA and the Police and Criminal Evidence Act 1984 (PACE).[211] Applications may

206. CICA, §§ 13–14, 17 (UK).

207. *Id.* §§ 13–14; JP Morgan Chase Bank Nat'l Ass'n v. Dir. of the Serious Fraud Off. [2012] EWHC (Admin) 1674 [25](ii), [2012] Lloyd's Rep. F.C. 655 (Eng.); R (Hafner) v. Sec'y State for Home Dep't [2006] EWHC (Admin) 1259 [33], [2007] 1 WLR 950 (Eng.); *see* United States v. Vilar, No. S305–CR–621 (KMK), 2007 WL 1075041, at *11–*12 (S.D.N.Y. Apr. 4, 2007) (elaborating *ex ante* UK MLA protections).

208. R (Abacha) v. Sec'y of State for the Home Dep't (No. 2) [2001] EWHC (Admin) 787 [48] (Eng.); *see* R (Terra Servs. Ltd.) v. Nat'l Crime Agency [2020] EWHC (Admin) 1640 [67]–[69], [2021] 1 WLR 1 (Eng.); R (Energy Fin. Team Ltd.) v. Bow St. Magistrates' Court [2005] EWHC (Admin) 1626 [11], [2006] 1 WLR 1316 (Kennedy, L.J.) (Eng.). *Contra* R v. Dir. of Serious Fraud Off. Ex p K.M. CO/3263/97, [1998] EWHC J0407-4, *30–*1 (QB, Apr. 7, 1998) (Eng.) (noting UKCA may face "[c]onsiderable difficulties" during initial "inquiries into [a r]equest").

209. *Terra Servs. Ltd.* [2020] EWHC (Admin) 1640 [56]–[66]; Gross v. Southwark Crown Court CO/1759/98, [1998] Lexis Citation 2837 (QB, July 24, 1998) (Eng.).

210. Police and Criminal Evidence Act 1984, c.60, § 9, sch. 1 (Eng. & Wales) [hereinafter PACE]; UK FACT SHEET, *supra* note 36, at 2; ZANDER, *supra* note 187, §§ 2-23–2-41. Production orders are available for MLA. R (Van Der Pijl) v. Sec'y of State for the Home Dep't [2014] EWHC (Admin) 281 [65], [98], [2014] Lloyd's Rep. F.C. 362; (Eng.); R (Sec'y of State for the Home Dep't) v. Southwark Crown Court [2013] EWHC (Admin) 4366 [26]–[33], [2014] 1 WLR 2529 (Eng.); *e.g.*, R (River East Supplies Ltd.) v. Crown Court at Nottingham [2017] EWHC (Admin) 1942 [2], [8], [2017] 4 WLR 135 (Eng.); *see* R (NTL Grp. Ltd.) v. Ipswich Crown Court [2002] EWHC (Admin) 1585, [2003] QB 131 (Eng.) (production order against service provider). *See generally Energy Fin. Team* [2005] EWHC (Admin) 1626, [24](1)–(2) (noting, in the context of executing an MLA request, that less intrusive methods for obtaining data are preferred).

211. CICA, §§ 13(1), 14, 15(2), 17; PACE § 9, sch. 1; Criminal Procedure Rules 2020, SI 2020/759, r. 47.10 (Eng.) [hereinafter CPR]; *e.g.*, Brookfield Aviation Int'l Ltd. v. Guildford Crown Court [2015] EWHC (Admin) 3465 [8] (Eng.); R (Ahsan) v. Gov't of the United States of America [2008] EWHC (Admin) 666 [8] (Eng.).

normally be obtained without notice to the provider.[212] They must evidence "reasonable grounds" of applicable matters, such as that the data will be of substantial value to the particular investigation,[213] although courts will conduct a "more circumscribed" assessment when data is sought through MLA.[214]

Service providers may conceivably oppose production orders before handing over data, albeit on limited grounds.[215] Potentially, an underlying target could also object, but they will not be aware of the application or even the resulting order unless informed by their provider, who may be requested to keep it confidential.[216] After the order is issued and executed, the data collected should be given to UKCA,[217] which should review then promptly transit that data to OIA,[218] so long as certain assurances have been given,[219] such as that the data will not be used to facilitate a prosecution resulting in the death penalty.[220] At

---

212. *See* CPR, r. 47.5. Exceptions apply—e.g. legally privileged materials—for which notice is normally required. *Id.*; PACE, sch. 1, paras. 7–11.

213. PACE, sch. 1, para. 2(a)(iii); ZANDER, *supra* note 187, §§ 2-26–2-28.

214. *Van der Pijl* [2014] EWHC (Admin) 281 [82]; *see Energy Fin. Team* [2005] EWHC (Admin) 1626 [11]–[17].

215. PACE, sch. 1; CPR, r. 47.8; ZANDER, *supra* note 187, §§ 2-26–2-28; *e.g.*, R (British Sky Broad. Ltd.) v. Comm'r of Police of Metropolis [2014] UKSC 17 [18], [33], [2014] AC 885 (appeal taken from Eng.).

216. ZANDER, *supra* note 187, §§ 2-36–2-37; *see* Maria Piggin, *Revenue Assistance*, 159 NEW L. J. 106, 106, (2009).

217. Transmission between central authorities is required. US–UK MLAT, *supra* note 61, at art. 2(4); NICHOLLS, MONTGOMERY, KNOWLES, DOOBAY & SUMMERS, *supra* note 68, ¶ 19.122 (citing CICA, Explanatory Notes ¶ 65); *e.g.* U.K. v. U.S., 238 F.3d 1312, 1316–17 (11th Cir. 2001); *cf.* CICA, § 19.

218. JP Morgan Chase Bank Nat'l Ass'n v. Dir. of the Serious Fraud Off. [2012] EWHC (Admin) 1674 [52], [72](ii), [2012] Lloyd's Rep. F.C. 655 (Eng.); R (Abacha) v. Sec'y of State for the Home Dep't (No. 2) [2001] EWHC (Admin) 787 [17] (Eng.); *see* Gross v. Southwark Crown Court CO/1759/98, [1998] Lexis Citation 2837 (QB, July 24, 1998) (Eng.) (referring to UKCA's transmission role as merely "a conduit pipe").

219. UK MLA GUIDELINES, *supra* note 196, at 26–27; *e.g.*, R (Evans) v. Dir. of the Serious Fraud Off. [2002] EWHC (Admin) 2304 [22]–[24], [2003] 1 WLR 299 (QB) (Eng.). *See generally* HM GOV'T, OVERSEAS SECURITY AND JUSTICE ASSISTANCE (OSJA): HUMAN RIGHTS GUIDANCE (2017) (providing general guidance on how to uphold human rights when providing assistance to foreign states, including through the use of assurances).

220. Elgizouli v. Sec'y of State for the Home Dep't, [2020] UKSC 10 [26], [2021] AC 937 (Lord Kerr dissenting but not on this point) (appeal taken from Eng.).

each of these UK steps, there is residual discretion to decline to progress a request,[221] although this is seldom exercised.[222]

The main method available to persons seeking to object to claimed rights breaches in the UK at this point is through judicial review.[223] This procedure is distinct from opposing a PACE application directly, although a decision to grant a PACE application may be at the heart of a judicial review application.[224] Applicants may seek judicial review of decisions made by those exercising public functions,[225] such as decisions to provide MLA to a foreign state.[226] Indeed, judicial review of each of the above UK MLA stages has been sought,[227] with occasional success.[228] While establishing 'standing'—i.e., a "sufficient interest" in the

221. *Abacha (No 2)* [2001] EWHC (Admin) 787 [1].

222. R (Elgizouli) v. Sec'y of State for the Home Dep't [2020] EWHC (Admin) 2516 [47], [2021] 3 All ER 247 (Eng.); UK MLA GUIDELINES, *supra* note 196, at 15; Victoria Ailes, *Mutual Legal Assistance and Other European Council Framework Decisions*, *in* EXTRADITION AND MUTUAL LEGAL ASSISTANCE HANDBOOK 147 ¶ 15.52 (John R.W.D. Jones & Rosemary Davidson eds., 2010); *e.g.*, R (BSG Res. Ltd.) v. Dir. of Serious Fraud Off. [2015] EWHC (Admin) 1813 [3] (discretion at authorization) (Eng.); Zardari v. Sec'y of State for the Home Dept (No. 2) [2001] EWHC (Admin) 275 [19], [23], [30]–[31] (Eng.) (discretion before transmission back).

223. *See* R (Energy Fin. Team Ltd.) v. Bow St. Magistrates Court [2005] EWHC (Admin) 1626 [24](9), [2006] 1 WLR 1316 (Eng.).

224. *E.g.*, R (Terra Servs. Ltd.) v. Nat'l Crime Agency [2020] EWHC (Admin) 1640 [3], [2021] 1 WLR 1 (Eng.).

225. *See generally* HARRY WOOLF, S.A. DE SMITH, JEFFERY L. JOWELL, CATHERINE M. DONNELLY & IVAN HARE, DE SMITH'S JUDICIAL REVIEW ¶ 1–001 (8th ed. 2018) [hereinafter DE SMITH'S].

226. *E.g.*, R (Abacha) v. Sec'y of State for the Home Dep't (No. 1) [2001] EWHC (Admin) 424 (Eng.).

227. *E.g.*, *id.* (UKCA decision to authorize request); R v. Sec'y of State for the Home Dep't Ex p S.p.A. [1997] 1 WLR (QB) 743, 755, 758 (Eng.) (UKCA referral to law enforcement); *Terra Servs. Ltd.* [2020] EWHC (Admin) 1640 [3] (law enforcement decision to seek order); Marlwood Com. Inc. v. Kozeny [2004] EWCA (Civ) 798, [2005] 1 WLR 104 (Eng.) (other law enforcement decision); R (Van der Pijl) v. Crown Court at Kingston [2012] EWHC (Admin) 3745 [1], [2013] 1 WLR 2706 (Eng.) (court issuance of order); Gross v. Southwark Crown Court CO/1759/98, [1998] Lexis Citation 2837 (QB, July 24, 1998) (Eng.) (UKCA transmission back).

228. *E.g.*, *Van der Pijl* [2012] EWHC (Admin) 3745 [91]–[94]; R v. Sec'y of State for the Home Dep't Ex p K.M. CO/3263/97, [1998] EWHC J0407-4, at *24 (QB, Apr. 7, 1998) (Eng.); *Gross* CO/1759/98; R v. Southwark Crown Court, Ex p Defries CO/283/95, [1995] Lexis Citation 1867 (Eng.); *see* Superior Import / Export Ltd. v. Comm'rs for Her Majesty's Revenue and Customs [2017] EWHC (Admin) 3172 [85] (Eng.).

decision under review—is a threshold criterion for seeking judicial review,[229] US targets of MLA requests would "undoubtedly" have standing.[230] Several further hurdles to judicial review in this context will however likely be fatal. Practically, judicial review would serve little purpose after transmission of data to the OIA, but, given the confidentiality of MLA, a target is unlikely to be able to have sufficient knowledge to bring a timely challenge in UK courts.[231] Moreover, proceeding to a full judicial review hearing requires permission of the court,[232] but judicial review of investigatory steps, such as decisions to provide MLA or obtain evidence, is rarely entertained.[233] Additionally, such decisions will typically be reviewed on strict *Wednesbury* grounds,[234] under which a decision will be set aside only if it was "so unreasonable that no reasonable authority could ever have come to it."[235] UK courts exercise even further restraint in "the

229. DE SMITH'S, *supra* note 225, ¶¶ 2-07 to 2-10.

230. R v. Cent. Crim. Ct. Ex p Propend Fin. Prop. Ltd. [1996] 2 Cr. App. R. (QB) 26, 29 (Eng.) ("The applicants, who … are parties concerned in the Australian investigation . . . undoubtedly have *locus* to mount these challenges."). *See generally* R (Good Law Project Ltd.) v. Sec'y of State for Health & Social Care [2021] EWHC (Admin) 346 [96], [2021] PTSR 1251 (Eng.) ("Since the early 1980s, the courts of England and Wales have generally adopted a liberal approach to the question of standing.").

231. *See* sources cited *supra* note 199.

232. DE SMITH'S, *supra* note 225, ¶¶ 16-044 to 16-054.

233. *E.g.*, R (Energy Fin. Team Ltd.) v. Bow St. Magistrates' Court [2005] EWHC (Admin) 1626 [24](9), [2006] 1 WLR 1316 (Eng.). *See generally* R (Unaenergy Grp. Holding) v. Dir. of Serious Fraud Off. [2017] EWHC (Admin) 600 [34] (iii) [2017] 1 WLR 3302 (Eng.) ("Challenges by way of judicial review to investigators in the conduct of an investigation have and should have a 'very high hurdle to overcome' and will be entertained only in exceptional circumstances.") (citation omitted).

234. Associated Provincial Picture Houses Ltd. v. Wednesbury Corp. [1948] 1 KB (CA) 223 (Eng.); *e.g.*, Fawwaz v. Sec'y of State for the Home Dept. [2015] EWHC (Admin) 166 [69] (Eng.); JP Morgan Chase Bank Nat'l Ass'n v. Dir. of the Serious Fraud Off. [2012] EWHC (Admin) 1674 [55], [2012] Lloyd's Rep. F.C. 655 (Eng.); R. Sec'y of State for the Home Dep't Ex p Finninvest S.P.A. [1997] 1 WLR 743, 757 (Eng.). *See generally* DE SMITH'S, *supra* note 225, ¶¶ 11-087 to 11-103 ("The default position is still, at the time of writing, that of the *Wednesbury* formulation.").

235. *Wednesbury* [1948] 1 KB at 230. This judgment dismissed a judicial review application by a movie theater seeking a declaration that a local authority condition that the theater could not admit children on Sundays was "unreasonable and that in consequence it was ultra vires," i.e., outside the authority's powers. *Id.* at 226–28. It provided the now seminal reasoning, quoted above, that courts will ordinarily review the 'reasonableness' of a public authority

context of mutual assistance."[236] They "take on trust" that a requesting state has acted lawfully and reasonably in making the request, absent "compelling" proof otherwise.[237] A claim that the US has breached, or may breach, a target's Fourth Amendment rights would be met by a UK court responding that this is "a matter for the requesting state."[238] In justifying this, UK courts have suggested that "it would normally be expected that a suspect would have the right to contest evidence in the requesting country."[239]

There is normally no way for US persons to directly object to MLA in UK courts on the basis that their digital privacy rights were breached. Because they are physically outside the UK, they will be barred from raising Article 8 or other ECHR claims before UK courts due to the "primarily territorial" interpretation given to the ECHR's Article 1 jurisdiction clause.[240] The ECtHR has held that the ECHR applies extraterritorially only

---

decision on narrow grounds only. It is the most famous (non-US) common law judicial review judgment in the world. *See, e.g.*, Michael Fordham, *Wednesbury*, 12 JUD. REV. 226, 226 (2007) ("No judicial review case goes by without [*Wednesbury*] being mentioned. Everybody knows its name. Nobody reads it any more. And nobody dare cite it to a judge: we know about grandmothers and egg-sucking.").

236. *Van der Pijl* [2012] EWHC (Admin) 3745 [81]–[82].

237. Malabu Oil & Gas Ltd. v. Dir. of Public Prosecutions [2016] Lloyd's Rep. F.C. 108 (CC) [43]–[44] (Eng.); *JP Morgan* [2012] EWHC (Admin) 1674 [53], [66], [72].

238. R v. Sec'y of State for the Home Dep't Ex p Zardari CO/0345/98, [1998] Lexis Citation 4659 (QB, Mar. 11, 1998) (Eng.); *see JP Morgan* [2012] EWHC (Admin) 1674 [52]–[54]; Calder v. Her Majesty's Advocate [2006] HCJAC 62, (2007) JC 4 [31] (Scot.); R (Abacha) v. Sec'y of State for the Home Dep't (No. 2) [2001] EWHC (Admin) 787 [27], [44] (Eng.); *see also* Gov't of India v. Quattrocchi [2004] EWCA (Civ) 40 [27] (Eng.) (rejecting attempt "to re-run or revisit the decisions taken by the Indian authorities", noting court was not equipped "either in terms of evidence or . . . knowledge of the Indian law").

239. *Abacha (No 2)* [2001] EWHC (Admin) 787 [50] (citing *Zardari* CO/0345/98 (Lord Bingham, C.J.)); *see Fawwaz* [2015] EWHC (Admin) 166 [61]. *But see* Marlwood Com. Inc. v. Kozeny [2004] EWCA (Civ) 798 [45], [2005] 1 WLR 104 (Eng.) ("[Q]uestions [may arise] as to whether the law of the foreign jurisdiction could be safely left to determine questions, for instance of admissibility.").

240. Al-Skeini v. United Kingdom [GC], 2011-IV Eur. Ct. H.R. 99 ¶ 131; *see* R (Al-Skeini) v. Sec'y of State for Def. [2007] UKHL 26 [58]–[59], [2008] AC 153 (appeal taken from Eng.); DE SMITH'S, *supra* note 225, ¶ 3-108. *See generally* ECHR, *supra* note 9, at art. 1 ("The High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in … [the ECHR].").

"exceptionally," with a handful of narrow circumstances recognized.[241] Although there is no authority from the ECtHR directly addressing when jurisdiction arises in the digital arena,[242] in 2015, the UK Investigatory Powers Tribunal ruled in *Human Rights Watch Inc v. Secretary of State for the Foreign & Commonwealth Office* that the UK owed "no obligation[s] under Article 8" to persons physically outside UK territory with respect to their electronic communications.[243] In 2017, the High Court of England and Wales rejected an Article 8 objection to a UK decision to provide MLA to Northern Cyprus because the claimant, then in Northern Cyprus, was not "within the jurisdiction of the UK for the purposes of the ECHR."[244] Other UK judgments considering ECHR Article 1 take the same narrow approach,[245]

---

241. *Al-Skeini*, 2011-IV Eur. Ct. H.R. 99 ¶¶ 130–42; Marko Milanovic, *Jurisdiction and Responsibility: Trends in the Jurisprudence of the Strasbourg Court*, *in* THE EUROPEAN CONVENTION ON HUMAN RIGHTS AND GENERAL INTERNATIONAL LAW 97, 102 (Anne van Aaken & Iulia Motoc eds., 2018) [hereinafter Milanovic, *Jurisdiction*].

242. *See* BVerfG, 1 BvR 2835/17, May 19, 2020 [97] (Ger.), http://www.bverfg.de/e/rs20200519_1bvr283517en.html; Kathryn Wilson, *The European Convention on Human Rights and the Investigatory Powers Tribunal: Rationalising a Law unto Itself?*, 23 TRINITY COLL. L. REV. 129, 144 (2020); Francesca Bignami & Giorgio Resta, *Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance*, *in* COMMUNITY INTERESTS ACROSS INTERNATIONAL LAW 357, 376 (Eyal Benvenisti & Georg Nolte eds., 2018).

243. Human Rights Watch Inc. v. Sec'y of State for the Foreign & Commonwealth Off. [2016] UKIPTrib15_165-CH [56]–[61]; *see* Lea Raible, *Human Rights Watch v. Secretary of State for the Foreign and Commonwealth Office: Victim Status, Extraterritoriality and the Search for Principled Reasoning*, 80 MODERN L. REV. 510, 518 (2017) (viewing this as "unsurprising . . . if only because the ECtHR case law is inconclusive at best"); *see also* Privacy Int'l v. Sec'y of State for Foreign and Commonwealth Affairs [2016] UKIPTrib 14_85-CH [48]–[53] (assuming a similar approach), *rev'd on other grounds*, Privacy Int'l v. Investigatory Powers Tribunal [2021] EWHC (Admin) 27, [2021] QB 936 (Eng.).

244. R (Akarcay) v. Chief Constable of the West Yorkshire Police [2017] EWHC (Admin) 159 [7]–[8], [35]–[36] (Eng.).

245. R (Plan B Earth) v. The Prime Minister [2021] EWHC (Admin) 3469 [61] (Eng.); Elgizouli v. Sec'y of State for the Home Dep't [2020] UKSC 10 [68], [116] (Lord Kerr dissenting but not on this point), [2021] AC 937 (appeal taken from Eng.); R (Sandiford) v. Sec'y of State for Foreign & Commonwealth Affairs [2014] UKSC 44 [21]–[34], [2014] 1 WLR 2697 (appeal taken from Eng.); S1 v. Sec'y of State for the Home Dep't [2016] EWCA Civ 560, [2016] 3 CMLR 37 [102]; R (Zagorski) v. Sec'y of State for Bus., Innovation & Skills [2010] EWHC (QB) 3110 [57], [2011] HRLR 6 (Eng.).

including against US persons specifically,[246] apparently regardless of any pre-existing UK ties they may have,[247] in contrast with the US approach.[248] It is unlikely that equivalent protections would apply under common law.[249] Indeed, the recent Scottish judgment referred to above was doubted on appeal.[250] Alternatively, although beyond the scope of this article, data protection claims may be available.[251]

3. Subsequent US Data Use

Once OIA receives the requested data from UKCA, it will review and then forward it to the requesting US law enforcement officer.[252] Both countries follow what has been called the 'rule of specialty' in MLA, meaning, absent further consent, MLA evidence may be used only for the proceedings for which it was sought.[253] Within such proceedings, however, US law enforcement have almost free reign.

---

246. *Zagorski* [2010] EWHC (QB) 3110 [57].

247. Khan v. United Kingdom, App. No. 11987/11, 58 Eur. H.R. Rep. SE15 ¶ 26 (2014). *But see* M.N. v. Belgium [GC], App. No. 3599/18 ¶ 115 (Mar. 5, 2020), https://hudoc.echr.coe.int/fre?i=001-202468; *Human Rights Watch* [2016] UKIPTrib15_165-CH [58] (both implying "pre-existing ties" with an ECHR member state may be relevant).

248. *See supra* text accompanying notes 172–173.

249. Hughes, *supra* note 134, at 92; *see* Ilic, *supra* note 148, at 33–34.

250. BC v. Chief Constable of the Police Serv. of Scot. [2020] CSIH 61 [75]–[89], [124], [140], (2021) SC 265 (Scot.); *see supra* text accompanying note 133.

251. *See supra* text accompanying notes 148–151. These include basic data protection rights each state has agreed to extend to the others' nationals pursuant to the international 'Umbrella Agreement' between the EU and United States. Agreement Regarding Law Enforcement Exchange and Protection of Information, US–EU, June 2, 2016, T.I.A.S. No. 17-201 [hereinafter Umbrella Agreement]. While the UK is no longer party to the Umbrella Agreement following Brexit, *see* EUROPEAN UNION COMMITTEE, BREXIT: THE EU DATA PROTECTION PACKAGE ¶ 61 (2017), the US and UK "have agreed to apply [its] safeguards in the MLA context as a matter of policy, and wish to make [its] provisions legally binding for MLA purposes as soon as possible." R (Elgizouli) v. Sec'y of State for the Home Dep't [2020] EWHC (Admin) 2516 [19] n.2, [2021] 3 All ER 247.

252. Snow, *supra* note 192, at 228.

253. US–UK MLAT, *supra* note 61, at art. 7(2); U.S JUSTICE MANUAL, *supra* note 192, at §§ 9–13.512; UK MLA GUIDELINES, *supra* note 196, at 6–7. While the United States applies this principle inconsistently, *see* Snow, *supra* note 192, at 225 n.62, it is "an absolute prohibition" in the UK CICA § 9(2); Tchenguiz v. Dir. of the Serious Fraud Off. [2014] EWCA (Civ) 1409 [63], [66](ii)

Normally, a US person could seek exclusion of evidence obtained in breach of their digital privacy rights under the Fourth Amendment's exclusionary rule,[254] which is its "principal judicial remedy."[255] The Fourth Amendment typically requires US law enforcement to act reasonably and obtain a warrant, which must be particularized and backed by probable cause,[256] before conducting a search or seizure infringing on reasonable expectations of privacy.[257] US courts increasingly recognize reasonable expectations of privacy over much electronic data, including the contents of emails held by service providers.[258] The exclusionary rule makes evidence obtained in breach of these obligations generally inadmissible.[259] It is "designed to safeguard Fourth Amendment rights generally through its deterrence effect."[260] It applies to evidence obtained directly from an illegal search and

---

(citing Gohil v. Gohil [2012] EWCA (Civ) 1550 [36]–[42], [2013] 2 WLR 1123). *See generally* BOISTER, *supra* note 2, at 321 (outlining the rule of specialty in MLA).

254. United States v. Leon, 468 U.S. 897, 909–10 (1984); Mapp v. Ohio, 367 U.S. 643, 650–60; Weeks v. United States, 232 U.S. 383, 398 (1914).

255. Utah v. Strieff, 579 U.S. 232, 237 (2016); *see* Herring v. United States, 555 U.S. 135, 153 (2009) (Ginsburg, J., dissenting) ("The exclusionary rule, it bears emphasis, is often the only remedy effective to redress a Fourth Amendment violation."); *Mapp*, 367 U.S. at 651–52 ("[T]he exclusionary rule is an essential ingredient of the Fourth Amendment.").

256. Kentucky v. King, 563 U.S. 452, 459 (2011); *see* Illinois v. Gates, 462 U.S. 213, 230–41 (1983) ("Probable cause is a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules.").

257. Kyllo v. United States, 533 U.S. 27, 31–35 (2001); *see* Grady v. North Carolina, 575 U.S. 306, 310 (2015) ("The Fourth Amendment prohibits only unreasonable searches. The reasonableness of a search depends on the totality of the circumstances."). *See generally* Brigham City v. Stuart, 547 U.S. 398, 403 (2006) ("[T]he ultimate touchstone of the Fourth Amendment is 'reasonableness.'").

258. Carpenter v. United States, 138 S. Ct. 2206, 2219–22 (2018); United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010); *see also* H.R. REP. NO. 114–528, at 9 (2016) (noting that it has been DOJ policy since 2013 to "us[e] warrants for email in all criminal cases"). *See generally* Riley v. California, 573 U.S. 373, 393–401 (2014) (holding that law enforcement "must generally secure a warrant" before searching cell phone or similar device data).

259. *Mapp*, 367 U.S. at 655. Exceptions apply, including for evidence obtained through "objectively reasonable reliance on a subsequently invalidated search warrant." *Leon*, 468 U.S. 922; *see also Herring*, 555 U.S. at 139–47 (further detailing exceptions).

260. *Herring*, 555 U.S. at 139–40.

seizure as well as "fruit of the poisonous tree," meaning later-discovered evidence "derivative of an illegality."[261]

The exclusionary rule will almost always be inapplicable in the MLA context, however,[262] because, "as a deterrent sanction, [it] is not applicable where . . . a foreign government commits the offending act."[263] Both direct and derivative MLA evidence are instead normally admissible regardless of rights breaches under what has been called the "international silver platter" doctrine.[264] Breaches of UK law when executing a US MLA request will not normally displace the application of this doctrine.[265] Even if OIA's initial actions in requesting MLA were unlawful, US courts would be slow to hold that the UK government's subsequent acquisition of that evidence was derivative of that

261. Wong Sun v. United States, 371 U.S. 471, 488 (1963); Segura v. United States, 468 U.S. 796, 804 (1984).

262. *E.g.*, United States v. Evtimov, No. 14-CR-131–4, 2016 WL 1181828, at *3–*5 (ND. Ill. Mar. 28, 2016); United States v. Omar, Crim. No. 09–242 (MJD/FLN), 2012 WL 2277821, at *2–*3 (D. Minn. June 18, 2012); United States v. Adler, 605 F. Supp. 2d 829, 837–38 (W.D. Tex. 2009).

263. United States v. Janis, 428 U.S. 433, 455 n.31 (1976) (citing United States v. Stonehill, 274 F. Supp. 420 (S.D. Cal. 1967)); *e.g.*, United States v. Odoni, 782 F.3d 1226, 1237–40 (11th Cir. 2015). *But cf. Herring*, 555 U.S. at 152–53 (Ginsburg, J., dissenting) (noting "the [exclusionary] rule also serves other important purposes" beyond deterrence).

264. United States v. Stokes, 726 F.3d 880, 890 (7th Cir. 2013); United States v. Lee, 723 F.3d 134, 139 (2d Cir. 2013); United States v. Emmanuel, 565 F.3d 1324, 1330 (11th Cir. 2009); Prabhu, Berrang & Dickey, *supra* note 45, at 177–79. Under the international silver platter doctrine, "if foreign police independently search an American citizen abroad under standards that would not have met fourth amendment requirements if conducted by U.S. authorities, the evidence acquired in that search could be admitted in a U.S. court." Caitlin T. Street, *Streaming the International Silver Platter Doctrine: Coordinating Transnational Law Enforcement in the Age of Global Terrorism and Technology*, 49 COLUM. J. TRANSNAT'L L. 411, 433 (2011). This doctrine is similar to the now defunct (domestic) 'silver platter doctrine', by which evidence supplied to federal law enforcement by their state equivalents was generally admissible and not subject to exclusion. *See* Elkins v. United States, 364 U.S. 206, 208, 215–17 (1960) (ruling that the silver platter doctrine should no longer apply in these domestic contexts). Although the domestic silver platter doctrine has long been abolished, its international counterpart remains in full force. *See generally Lee*, 723 F.3d at 139 n.3 (discussing international silver platter doctrine's history and rationale in the context of its domestic counterpart); LAFAVE, *supra* note 187, § 1.8(h) (similar).

265. United States v. Umeh, 646 F. App'x 96, 100 (2d Cir. 2016); *see* United States v. Lee, 723 F.3d 134, 137 (2d Cir. 2013).

illegality.[266] The main exception to the doctrine is where US law enforcement were so substantially involved that the acquisition became a "joint venture" with foreign officials.[267] Nonetheless, in the rare scenarios that the Fourth Amendment is then applied, US courts have held that only the Fourth Amendment's reasonableness requirement will apply abroad, so warrants are not necessary.[268] A second, and less coherently articulated, residual exception applies where acts of foreign law enforcement 'shock the conscience.'[269] This is an extremely high bar, typically triggered only by allegations of "torture or other truly heinous conduct."[270] So long as they do not literally resort to torture or equivalent acts, foreign law enforcement officials can apparently freely violate a defendant's privacy or other rights under the guise of fulfilling an MLA request for US law enforcement without this second exception being triggered.[271]

4. Reciprocal UK Requests

The reciprocal position, where US persons' data is sought by the UK through MLA, can be outlined briefly. Overall, although *ex ante* statutory protections constrain UK officials' acts in principle, the UK's own acts when seeking MLA data—first making a request and subsequently receiving and deploying data in criminal proceedings—provide limited protections in practice for

---

266. *E.g.*, United States v. Vilar, No. S305–CR–621 (KMK), 2007 WL 1075041, at *59 (S.D.N.Y. Apr. 4, 2007).

267. *See* Prabhu, Berrang & Dickey, *supra* note 45, at 177–78; *cf. Lee*, 723 F.3d at 140. The doctrine may not apply to data seized, but not searched, by foreign law enforcement. *Odoni,* 782 F.3d at 1239–40. However, it is U.K. practice to search data before providing it through MLA. *Id.*

268. *In re* Terrorist Bombings of U.S. Embassies in East Africa, 552 F.3d 157, 167–73 (2d Cir. 2008); *Stokes*, 726 F.3d at 891–93; Prabhu, Berrang & Dickey, *supra* note 45, at 179; *see* Kerr, *supra* note 166, at 297–301; LAFAVE, *supra* note 187, § 1.8(h).

269. Prabhu, Berrang & Dickey, *supra* note 45, at 178 n. 46. There may be a circuit divide on whether this exception arises under the Fourth Amendment, United States v. Rojas, 812 F.3d 382, 397 (5th Cir. 2016), or the Fifth Amendment's Due Process clause. United States v. Getto, 729 F.3d 221, 229 (2d Cir. 2013).

270. United States v. Getto, No. 09 CR 667 HB, 2010 WL 3467860, at *3 (S.D.N.Y. Aug. 25, 2010), aff'd, 729 F.3d 221 (2d Cir. 2013); *e.g.*, United States v. Fernandez-Caro, 677 F. Supp. 893, 895 (S.D. Tex. 1987); Currie, *Human Rights*, *supra* note 19, at 178; Street, *supra* note 264, at 434 n.91.

271. *See, e.g.*, *Getto*, 729 F.3d at 229–30 (citing Rochin v. California, 342 U.S. 165, 172 (1952)).

digital privacy rights. While methods to exclude evidence remain theoretically available to US persons,[272] they are applied narrowly.[273] US persons are relatively worse off than their UK counterparts, given that under existing UK authority the UK apparently owes no Article 8 obligation to US persons.[274] Even when such persons are brought to the UK for prosecution, thus entering its ECHR jurisdiction,[275] they will likely be barred from pursuing ECHR Article 8 claims arising from MLA conduct pre-dating their UK presence.[276]

US persons have few protections even at the second MLA stage, when UK MLA requests are executed in the US. Some *ex ante* protection is provided by the OIA and US legislation.[277] US MLA actions may theoretically be challenged on constitutional grounds but, as noted, no challenges have been successful.[278] Additionally, US courts appear to bar Fourth Amendment challenges to applications made for the contents of electronic communications during MLA. These applications are made under a combination of the SCA and enabling statutes.[279] They will often be issued without target notice,[280] and may expressly prohibit disclosure by the provider to the target.[281] This leaves only the

---

272. *E.g.,* R v. Okafor [1994] 3 All ER 742, 744–48 (CA) (Eng.).

273. *See infra* text accompanying notes 355–358.

274. *See supra* text accompanying notes 240–251.

275. R (Ismail) v. Sec'y of State for the Home Dep't [2016] UKSC 37 [32], [2016] 1 WLR 2814.

276. *See* Chagos Islanders v. United Kingdom, App. No. 35622/04, 56 Eur. H.R. Rep. SE15, ¶ 63 (2013). *See generally* Assanidze v. Georgia [GC], 2004-II Eur. Ct. H.R. 155 ¶ 137 ("[T]he state parties are answerable for any violation of the protected rights and freedoms of anyone within their 'jurisdiction' – or competence – at the time of the violation.").

277. Swire & Hemmings, *Visa Waiver*, *supra* note 82, at 735–36.

278. *See* sources cited *supra* note 202 and accompanying text.

279. SCA, 18 U.S.C. §§ 2701–2713 (2018); Foreign Evidence Request Efficiency Act, 18 U.S.C. § 3512 (2009); 28 U.S.C. § 1782 (2018); Funk, *supra* note 193, at 554–57; RESTATEMENT (FOURTH), *supra* note 202, at § 429 cmt. B; *e.g.*, *In re* United States for an Order Pursuant to 18 U.S.C. § 2703(D), Misc. Action No. 17–2682 (BAH), 2018 WL 1521772, at *1, n.1 (D.D.C. Mar. 8, 2018).

280. SCA, 18 U.S.C. §§ 2703(b), (c)(3), 2705; *e.g.*, *In re* United States, 665 F. Supp. 2d 1210, 1224 (D. Or. 2009).

281. SCA, 18 U.S.C. § 2705(b); *see In re* Subpoena 2018R00776, 947 F.3d 148 (3d Cir. 2020); United States v. Alahmedalabdaloklah, No. CR-12-01263-PHX-NVW, 2017 WL 2839645, at *8–9 (D. Ariz. July 3, 2017). *But see In re* Sealing & Non-Disclosure of Pen/Trap/2703(d) Orders, 562 F. Supp. 2d 876, 880 (S.D. Tex. 2008) ("Whether such a notice preclusion order would also prohibit a truthful response to an unsolicited customer inquiry is debatable."). Absent

service provider able to object.[282] Yet the provider can do so on limited grounds only; they apparently cannot vicariously assert a target's Fourth Amendment rights.[283] Even when targets attempt to bring challenges, US courts considering the issue have held that targets lack "Fourth Amendment standing" to challenge such SCA warrants prior to execution,[284] leaving targets with no way to then uphold their digital privacy rights.

B. The US–UK Agreement Enhances US Persons' Digital Privacy Rights

Protections for US persons' digital privacy rights—both *ex ante* and, most significantly, *ex post*—will be enhanced through the US–UK Agreement relative to MLA. These benefits outweigh potential downsides for US persons.

1. The Impact and Operation of CLOUD Act Agreements for US Persons

Where the US seeks UK data under the US–UK Agreement, the process will initially be similar to MLA. Each State has a "designated authority," through which requests must be

---

such a 'gagging order,' prohibiting disclosure to a target, US service providers increasingly will disclose to their customers as a matter of course. ANDERSON, *supra* note 41, ¶ 11.9; *e.g.*, In re Search of Info. Associated With One Acct. Stored at Premises Controlled by Facebook, Inc., No. 21-SC-1386 (GMH), 2021 WL 2302800, at *1 (D.D.C. June 4, 2021); United States v. Information Associated With Email Account (Warrant), 449 F.Supp.3d 469, 470 (E.D. Pa. 2020); Smith, *supra* note 160.

282. *See* cases cited *supra* note 281.

283. SCA, 18 U.S.C. § 2703(d); *e.g.*, Microsoft Corp. v. United States Dep't of Justice, 233 F. Supp. 3d 887, 915–16 (W.D. Wash. 2017). These approaches have been criticized. Jennifer Daskal, Symposium, *Notice and Standing in the Fourth Amendment: Searches of Personal Data*, 26 WM. & MARY BILL RTS. J. 437 (2017) [hereinafter Daskal, *Notice*]; *see* Aviv S. Halpern, Note, *Secret Searches: The SCA's Standing Conundrum*, 117 MICH. L. REV. 1697 (2019). *See generally* Alderman v. United States, 394 U.S. 165, 174 (1969) ("Fourth Amendment rights are personal rights which, like some other constitutional rights, may not be vicariously asserted.").

284. United States v. Info. Assoc. With Email Acct. (Warrant), 449 F. Supp. 3d 469, 473–76 (E.D. Pa. 2020); *In re* Search of Records, Info, & Data Associated with 14 Email Addresses Controlled by Google, LLC. 438 F. Supp. 3d 771, 774–75 (E.D. Mich. 2020); *see In re Search of Info. Assoc.,* No. 21-SC-1386 (GMH), 2021 WL 2302800, at *3 (D.D.C. June 4, 2021) (rejecting target challenge prior to execution of SCA warrants directed to Facebook and Twitter, referring to precedent prohibiting this as "clear").

channeled.[285] These designated authorities operate similarly to MLA central authorities.[286] This is underscored by the appointment of OIA by the US to serve in this new role.[287] Law enforcement will presumably work with the OIA to ensure that each request complies with the US–UK Agreement.[288] Unlike MLA, however, this first step will also include obtaining any local court order required under US law.[289] This section assumes that US law enforcement would channel CLOUD Act agreement requests through the SCA.[290]

At the second stage of this process—evaluation and execution of the request in a foreign state—CLOUD Act agreements chart a significantly different course.[291] OIA will no longer transmit a request to UKCA for UK law evaluation and execution; instead, OIA will directly serve the UK service provider with a US request, along with a certification it is issued under and in compliance with the US–UK Agreement and US law.[292] That provider will have a short period to review the request and provide the data or wiretap sought.[293] There are admittedly concerns with

285. US–UK AGREEMENT, *supra* note 4, at arts. 1(8), 5(5)–(12).

286. *See supra* text accompanying notes 193, 205.

287. AG Order No. 4877-2020, 85 Fed. Reg. 67446-01 (Oct. 23, 2020) (to be codified at 28 C.F.R. § 0.64–6); Dep't of Just. Off. Of the Insp.-Gen., Audit of the Criminal Division's Process for Incoming Mutual Legal Assistance Requests Audit Division 18–19 (21-097, July 2021), https://oig.justice.gov/sites/default/files/reports/21-097.pdf [hereinafter DOJOIG report].

288. US–UK AGREEMENT, *supra* note 4, at arts. 5(5)–(6).

289. *Id.* at arts. 1(11), 5(1).

290. *See, e.g.*, Robert J. Peters, Alicia D. Loy, Matthew Osteen, Joseph Remy & Justin Fitzsimmons, *Not an Ocean Away, only a Moment Away: A Prosecutor's Primer for Obtaining Remotely Stored Data*, 47 MITCHELL HAMLINE L. REV. 1072, 1094–95 (2021) (making a similar assumption). Daskal argues that additional new "explicit legal authority in U.S. law" would be needed for the US to issue requests to non-US service providers under the US–UK Agreement. Daskal, *Privacy and Security*, *supra* note 36, at 1041. I respond to this argument elsewhere. Cochrane, *supra* note 114, at 206–208. In any event, Daskal appears to acknowledge that the U.S. Congress could theoretically legislate for such authority.

291. *Cf.* discussion *supra* Sections II.A.2–II.A.3.

292. *See* US–UK Agreement, *supra* note 4.

293. This Article assumes any US timeframe would be similar to the UK. *See* COPOA, § 5(5) (providing a default period of seven days within which providers must respond to requests issued under COPOA); *see also* UK HOME OFFICE, IMPACT ASSESSMENT, POLICE, CRIME, SENTENCING AND COURTS BILL 7 (HO0383, 2021), https://publications.parliament.uk/pa/bills/cbill/58-01/0268/20210304%20HO0383%20-%20PCSC%20Overarching%20IA%20-

relying on service providers to conduct this review addressed separately below.[294] Taken together, however, these first two steps enhance digital privacy rights of US persons. Their data will no longer have been compelled pursuant to, first, a US MLA process without judicial oversight,[295] and, secondly, a UK process that denies them the protection of Article 8.[296] Instead, a US court will have independently evaluated the proposed request against statutory constraints,[297] as well as the US Persons' Fourth Amendment rights.[298] This provides relatively greater *ex ante* protections.

In any event, the greatest enhancement for US persons' digital privacy rights is at the final stage, through enhanced *ex post* protections. Data provided will be reviewed by OIA and then provided to the requesting law enforcement officer,[299] who is free to deploy it in criminal proceedings as if it were obtained domestically.[300] At this point under MLA, data is generally admissible under the international silver platter doctrine, severely limiting digital privacy rights.[301] Under CLOUD Act agreements, however, this doctrine should no longer apply, as US law enforcement will be in control of the entire evidence-collection process.[302] The Supreme Court clarified as early as 1960 that law

---

%20FINAL%20CLEAN%20(signed).pdf ("The [entire] COPO[A] process is expected to take in the order of 60 days and perhaps less.").

294. *See infra* text accompanying notes 468–491.

295. *See supra* text accompanying note 200.

296. *See* discussion *supra* Section II.A.2.

297. *See* Swire & Kennedy-Mayo, *supra* note 138, at 644–46 (outlining the Wiretap Act's "probable cause-plus" standard); Orin S. Kerr, Symposium, A User's Guide to the Stored Communications Act, and A Legislator's Guide to Amending It, 72 GEO. WASH. L. REV. 1208, 1214 (2004) (noting the SCA's "Fourth Amendment-like" protections here).

298. *But see infra* text accompanying notes 304–310.

299. *See* US–UK AGREEMENT, *supra* note 4, at arts. 6(1)–(2), 10(6).

300. *Cf. supra* text accompanying note 253 (referring to the 'rule of specialty' in MLA).

301. *See supra* text accompanying notes 262–271.

302. *See* United States v. Verdugo-Urquidez, 494 U.S. 259, 283 n.7 (1990) (Brennan, J., dissenting); *e.g.* United States v. Stokes, 726 F.3d 880 at 890–91 (7th Cir. 2013); *In re* Terrorist Bombings of U.S. Embassies in East Africa, 552 F.3d 157, 167 (2d Cir. 2008). *See generally* Boumediene v. Bush, 553 U.S. 723, 765 (2008) ("Even when the United States acts outside its borders, its powers are not absolute and unlimited but are subject to such restrictions as are expressed in the Constitution.") (citation omitted) (internal quotation marks omitted); Reid v. Covert, 354 U.S. 1, 6 (1957) (when the United States acts extraterritorially against U.S. persons, "the shield which the Bill of Rights and

enforcement cannot disclaim responsibility for breaches of rights in such circumstances.[303] Given the importance of this rule in vindicating the digital privacy rights of US persons, this shift is significant, providing markedly enhanced rights protection in practice.

2. Potential Downsides

The first potential downside arises from *how* the US will implement US–UK Agreement in US law. The above assumes the US would use a legal process equivalent to the SCA or Wiretap Act, but this is an open question.[304] The US–UK Agreement only requires that US requests for communications content use "a legal instrument issued under the domestic law of the Issuing Party,"[305] which must have a "reasonable justification, based on articulable and credible facts, particularity, legality, and severity."[306] CLOUD Act agreement requests targeting US persons would also need to comply with the Fourth Amendment.[307] Daskal, however, suggests that these requests would be "extraterritorial" under US law.[308] If so, the US may ultimately be able to lawfully target US persons using legal instruments with fewer protections than those provided by the SCA and Wiretap Act. Neither the US–UK Agreement nor the Fourth Amendment, as currently interpreted, require requests to have prior judicial approval or certain other warrant indicia.[309] Nonetheless, the US–UK Agreement is still a relative improvement compared with

---

other parts of the Constitution provide to protect [a person's] life and liberty should not be stripped away").

303. Elkins v. United States, 364 U.S. 206, 208, 215–17 (1960); *see supra* note 264.

304. *See supra* text accompanying note 290.

305. US–UK AGREEMENT, *supra* note 4, at arts. 1(11), 5(5)–(7), 10(2).

306. US–UK AGREEMENT, *supra* note 4, at art. 5(1).

307. *See supra* sources cited notes 188, 302 and accompanying text.

308. Daskal, *Privacy and Security*, *supra* note 36, at 1041; 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.crossborderdataforum.org/setting-the-record-straight-the-cloud-act-and-the-reach-of-wiretapping-authority-under-us-law/.

309. US–UK AGREEMENT, *supra* note 4, at art. 5(2) (permitting orders "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). As noted, under current interpretations, only the Fourth Amendment's reasonableness requirement applies abroad; its warrant requirement does not. *See supra* text accompanying note 268.

MLA for US persons: they benefit from, at least, the Fourth Amendment's reasonableness requirement and, in particular, the exclusionary rule.[310]

The second potential downside is the possibility of incidental collection of US persons' data through UK requests.[311] As noted, despite targeting and minimization procedures,[312] incidental collection is considered likely.[313] These procedures appear to allow broad scope for subsequent use of such data.[314] While potentially concerning, this still pales in significance to the benefits US persons receive. Ultimately, the full application of US law at all stages here is a significant gain for US persons' digital privacy rights compared with the partial application of US and UK laws under MLA.

C. UK Persons' Digital Privacy Rights Are Similarly Limited under MLA

UK persons also receive diminished protections for their digital privacy rights during MLA compared with domestic evidence collection.[315] In principle, the UK must act consistently with Article 8 in relation to anyone physically within UK territory.[316] UK persons however have very limited scope to uphold these rights in practice during MLA.[317] Overall, they are in a similar, albeit less severe, position to their US counterparts.

1. Initial UK Steps

Requests for communications content held by US service providers generally require a formal MLA request under CICA, the UK's main MLA statute.[318] These are normally initiated by UK law enforcement.[319] The requests are then reviewed by UKCA

310. *See supra* text accompanying notes 299–303.

311. *See* sources cited *supra* note 169 and accompanying text.

312. US–UK AGREEMENT, *supra* note 4, at arts. 4(3)–(4), 7.

313. *See* sources cited *supra* note 169.

314. *See* US–UK AGREEMENT, *supra* note 4, at arts. 7(3), 7(5).

315. *See* sources cited *supra* note 187.

316. Aston Cantlow & Wilmcote with Billesley Parochial Church Council v. Wallbank [2003] UKHL 37 [7], [2004] 1 AC 546 (appeal taken from Eng.).

317. *See infra* text accompanying notes 318–367.

318. CICA, § 7; UK MLA GUIDELINES, *supra* note 196, at 30; *see supra* text accompanying note 62; *cf.* R v. Redmond [2006] EWCA (Crim) 1744 [25], [2009] 1 Cr. App. R. 25.

319. CICA, § 7; Crime (International Co-operation) Act 2003 (Designation of Prosecuting Authorities) Order 2004, SI 1034/2004, ¶ 2 (Eng., Wales and N.

before transmission,[320] which will assess requests against CICA's threshold requirements.[321] This provides some *ex ante* protections for UK persons.

Like in the US, however, there is very little ability to meaningfully enforce these obligations in practice in the UK.[322] Court approval of requests is not required.[323] Judicial review of such steps "should be very rare."[324] UK law enforcement is under much less onerous obligations when issuing an MLA request than apply when they seek equivalent data using domestic processes.[325] The UK "duty of candour"—which requires disclosure of all relevant information, including potentially adverse information, in court applications[326]—does not apply to MLA requests.[327] Courts also accept that requests may be very broadly drafted.[328] As requests are confidential, targets are also very unlikely to know when a request is made.[329] To date, UK courts

---

Ir.); Alun Jones & Michael O'Kane, *Mutual Legal Assistance in the United Kingdom; The 2003 Statutory Scheme*, *in* JONES AND DOOBAY ON EXTRADITION AND MUTUAL ASSISTANCE 384, 394 (3d ed., Alun Jones & Anand Doobay eds., 2005).

320. CHRISTOPHER MURRAY & LORNA HARRIS, MUTUAL ASSISTANCE IN CRIMINAL MATTERS §§ 3.01, 3.12 (2000); CPS, *supra* note 199 ("A completed, authorised request (and supporting material) must be submitted to the [UKCA] for transmission.").

321. CICA, § 7(5); *Re* McIntrye [2018] NIQB 79 [31]–[33], [2020] NI 483 (N. Ir.); *e.g.*, R v. Foxley [1995] 2 Cr. Ap. R. (CA) 523, 532–36 (Eng.).

322. *See supra* text accompanying notes 198–204.

323. CICA, § 7; Alex Mills, *Crime (Overseas Production Orders) Act 2019: The Increasing Relevance of UK Investigatory Powers to those Advising Businesses and Individuals*, 9 J. INT'L BANKING & FIN. L. 624, 624 (2019).

324. R (Unaenergy Grp. Holding) v. Dir. of Serious Fraud Off. [2017] EWHC (Admin) 600 [24], [34](iii), [2017] 1 WLR 3302, (Eng.); *see also* sources cited *supra* note 233 and accompanying text.

325. *Unaenergy* [2017] EWHC (Admin) 600 [34](iii); *see* Mills, *supra* note 323, at 624 ("[I]t is difficult to challenge the issuing of a [MLA request] in the manner that a search warrant or production order issued in the U.K. could be challenged.").

326. *See* R (Haralambous) v. Crown Court at St. Albans [2018] UKSC 1 [25]–[27], [2018] AC 236 (appeal taken from Eng.).

327. *Unaenergy* [2017] EWHC (Admin) 600 [32], [34], [37], [53]; *McIntyre* [2018] NIQB 79 [43]–[45], [2020] NI 483 (N. Ir.); *see Foxley* [1995] 2 Cr. Ap. R. at 533–534 (discussing CICA's limited obligations).

328. R v. Sec'y of State for the Home Dep't Ex p Fininvest S.p.A. [1997] 1 WLR (QB) 743, 752–54 (Eng.); *e.g.*, Rea's (Winston Churchill) Application [2015] NICA (Civ) 8 [14]–[16], [2016] NI 203 (N. Ir.) (upholding a broad U.K. MLA request, noting "these matters are still at the 'investigation stage.'").

329. *See supra* text accompanying note 199.

have, at most, merely assumed, but never actually determined, that a decision to transmit an MLA request engages privacy rights protected by Article 8.[330] They have then readily concluded that any interference is justified.[331]

2. US Execution of UK Requests

OIA will initially review UK MLA requests for compliance with US law.[332] If satisfied, it will then forward the requests to US law enforcement to take forward.[333] As noted, requests for stored data are sought under a combination of the SCA and specific MLA statutes.[334] Communications content will be authorized by US courts, acting as "gatekeepers,"[335] only where "probable cause" is demonstrated.[336] As in the UK, US authorities have discretion to refuse assistance, but there is a strong presumption requests will be granted.[337] Nonetheless, the above steps provide some *ex ante* protections for UK persons. Notably, the SCA's privacy protections apply equally to US persons and foreigners.[338]

Ex post protections are however largely non-existent.[339] It is unlikely that UK persons will be aware when an SCA order is sought or be found to have standing to dispute it in any event.[340]

---

330. *McIntyre* [2018] NIQB 79 [51], [52](xi); *Winston Churchill* [2015] NICA (Civ) 8 [23]–[26]; R (BSG Res. Ltd.) v. Dir. of Serious Fraud Off. [2015] EWHC (Admin) 1813 [19]; *see Unaenergy* [2017] EWHC (Admin) 600 [37] (suggesting any Article 8 impact would be limited). *But see also Bloomberg v. ZXC* [2022] UKSC 2 (potentially indicating a more dangerous approach).

331. *McIntyre* [2018] NIQB 79 [51]; *Winston Churchill* [2015] NICA (Civ) 8 [25].

332. Matos v. Reno, No. 96 CIV. 2974 (MBM), 1996 WL 467519, at *2 (S.D.N.Y. Aug. 16, 1996); Swire & Hemmings, *Visa Waiver*, *supra* note 82, at 698–700, 735–36.

333. Swire & Hemmings, *Visa Waiver*, *supra* note 82, at 698–700, 735–36.

334. SCA, 18 U.S.C. §§ 2701–2713 (2018); Foreign Evidence Request Efficiency Act, 18 U.S.C. § 3512 (2009); 28 U.S.C. § 1782 (2018); *see supra* additional sources cited at note 279.

335. Funk, *supra* note 193, at 556–57.

336. *See supra* note 256.

337. Funk, *supra* note 193, at 557 (citing *In re* Premises Located at 840 140th Ave. NE, Bellevue, Wash., 634 F.3d 557, 571 (9th Cir. 2011)).

338. Suzlon Energy Ltd. v. Microsoft Corp., 671 F.3d 726, 729 (9th Cir. 2011); *see In re* Toft, 453 B.R. 186, 197–98 (Bankr. S.D.N.Y. 2011); Kerr, *supra* note 48, at 408.

339. *See infra* text accompanying notes 340–346.

340. *See supra* text accompanying note 284.

Service providers may object on limited grounds only.[341] Neither the requesting US law enforcement nor the authorizing US court will normally be concerned with whether the MLA request being executed complies with UK law.[342] Crucially, UK persons are also denied the main US tool for protecting digital privacy rights in this context, the Fourth Amendment, given *Verdugo-Urquidez*.[343] While the meaning of "substantial connections" remains debated,[344] *Verdugo-Urquidez* is commonly applied in the MLA context.[345] US courts have consistently held that non-US citizens who are not residents in the US simply "do not have standing" to pursue Fourth Amendment claims, even in the face of assumed unlawful conduct.[346]

---

341. *See supra* text accompanying note 283.

342. *See In re* Premises Located at 840 140th Ave. NE, Bellevue, Wash., 634 F.3d 557, 573 (9th Cir. 2011)*; In re* Commissioner's Subpoenas, 325 F.3d 1287, 1305 (11th Cir. 2003); Woods, *supra* note 42, at 666; *e.g.*, *In re* Request from Canada Pursuant to the Treaty Between the U.S. & Canada on Mut. Legal Assistance in Crim. Matters, 155 F. Supp. 2d 515, 519 (M.D.N.C. 2001).

343. United States v. Verdugo-Urquidez, 494 U.S. 259, 265–75 (1990); *see supra* text accompanying notes 172–173 and accompanying text (introducing and summarizing *Verdugo-Urquidez*).

344. United States v. Fantin, 130 F. Supp. 2d 385, 390–91 (W.D.N.Y. 2000); Kerr, *supra* note 166, at 308; Laura K. Donohue, *The Fourth Amendment in a Digital World*, 71 N.Y.U. ANN. SURV. AM. L. 553, 667 (2017). *Compare* Ibrahim v. Dep't of Homeland Sec., 669 F.3d 983, 996–97 (9th Cir. 2012) (holding petitioner established sufficient substantial connections through study at a U.S. university), *with id.* at 1002–04 (Duffy, J., dissenting) (disagreeing with majority on basis that the court would then "be hard pressed hard not to allow all alien students who studied in the United States and subsequently left the country to bring constitutional claims in our courts").

345. *E.g.*, United States v. Rojas, 812 F.3d 382, 397–98 (5th Cir. 2016); United States v. Emmanuel, 565 F.3d 1324, 1331–32 (11th Cir. 2009); United States v. Zakharov, 468 F.3d 1171, 1179 (9th Cir. 2006); *see* United States v. Defreitas, 701 F. Supp. 2d 297, 304 (E.D.N.Y. 2010) (noting this approach is "well settled"); Prabhu, Berrang & Dickey, *supra* note 45, at 177–78 (noting, when law enforcement seek overseas electronic data, "[a] predicate consideration, of course, are the voluntary [U.S.] connections" of the data subject). *See also* United States v. Hasbajrami, 945 F.3d 641, 665 (2d Cir. 2019) ("[A] person who does not have a Fourth Amendment-protected privacy interest in his communications, such as a foreign national resident abroad, does not acquire such an interest by reason of the physical location of the intercepting device.").

346. *E.g.*, United States v. Juarez, No. 1:16-CR-341-MHC-CMS, 2019 WL 2482167, at *3 (N.D. Ga. Jan. 11, 2019) ("Defendants have not disputed that at the time of their arrests, they were both citizens and residents of Guatemala, and they have presented no evidence that they had any voluntary attachment to the United States. As such, they do not have standing to assert a

3. Subsequent UK Data Use

Upon receipt of the requested data,[347] UKCA will provide the data to the requesting law enforcement officer, who can then deploy it in criminal proceedings, subject to standard admissibility rules,[348] as well as the rule of specialty.[349] Unlike the US position, an exclusion remedy remains theoretically available for UK persons whose Article 8 rights have been breached during MLA.[350] This may either be sought directly during criminal proceedings using a specific statutory provision of PACE, § 78,[351] or through judicial review.[352] While the ECHR only applies to its

---

constitutional challenge to the admission of this evidence."); United States v. Coke, No. 07 CR 971 RPP, 2011 WL 3738969, at *5 n.7 (S.D.N.Y. Aug. 22, 2011) ("Coke claims that the United States was engaged in a 'joint venture with law enforcement personnel of the Government of Jamaica to conduct a narcotics investigation of defendant Coke.' . . . Here, even if the Second Circuit had adopted the joint venture concept, Coke, as a non-citizen, has no standing to bring a Fourth Amendment claim."); *see* United States v. Guzman Loera, 24 F.4th 144, 157 (2d Cir. 2022) ("With respect to the Dutch Calls, neither Guzman nor the servers on which the calls were stored were located in the United States. Accordingly, the Dutch Calls were not subject to Fourth Amendment protections.").

347. MURRAY & HARRIS, *supra* note 320, § 5.44.

348. *See* CICA, Explanatory Notes ¶ 42 ("[E]vidence obtained from an overseas authority … is subject to the same provisions on admissibility of evidence as evidence obtained under normal domestic arrangements."); *e.g.*, R v. Iqbai [2002] EWCA (Crim) 2714 [8].

349. *See supra* text accompanying note 253.

350. *See supra* text accompanying note 262.

351. PACE § 78 provides a statutory power for courts to exclude prosecution evidence "if it appears to the court that, having regard to all the circumstances, including the circumstances in which the evidence was obtained, the admission of the evidence would have such an adverse effect on the fairness of the proceedings that the court ought not to admit it." *See generally* ZANDER, *supra* note 187, §§ 8-44–8-70 (discussing the history and operation of this provision and describing it as "the most used and arguably the most important section of [PACE]").

352. *E.g.*, R v. Knaggs [2018] EWCA (Crim) 1863 [168]–[171] (Eng.) (discussing possibility of exclusion of foreign-obtained criminal evidence using the statutory mechanism provided by § 78 of the PACE); R (Unaenergy Grp. Holding) v. Dir. of Serious Fraud Off. [2017] EWHC (Admin) 600 [10], [2017] 1 WLR 3302 (Eng.) (noting applicants had sought order through judicial review that UK law enforcement be required to return evidence obtained through MLA, thus ensuring it could not be used in any subsequent criminal proceedings). *But see also* R (*C*) v. Dir. of Pub. Prosecutions [2020] EWHC (Admin) 2967 [44], [2020] 4 WLR 158 (holding, where defendant does not challenge "the validity of [an EU MLA request] itself, but, rather, the use to which [its] product . . .

member states,[353] the ECtHR has recognized that reliance by a member state on evidence unlawfully obtained by a foreign state may breach that member's own ECHR obligations.[354] Compared with the ordinary US approach, however, a much less generous exclusion test applies in the UK and before the ECtHR.[355] Other than when procured through torture,[356] evidence obtained in breach of ECHR rights remains generally admissible.[357] Such evidence will be excluded only where, considering all the circumstances, its admission would breach a defendant's fair trial rights protected by Article 6.[358]

The rule of non-inquiry applied by UK courts further restricts the possibility of excluding MLA evidence.[359] Just as UK courts assume foreign states have acted lawfully and reasonably in

---

may be put in subsequent criminal proceedings", they should use PACE § 78), *aff'd sub. nom.*, R v. A, [2020] EWCA (Crim) 128, [2021] QB 791 (Eng.). A further remedy that "overlap[s]" with PACE § 78 is to seek to stay proceedings altogether for abuse of process. ZANDER, *supra* note 187, § 8-50.

353. Soering v. United Kingdom, 161 Eur. Ct. H.R. (ser. A) ¶ 86 (1989); *see* R (Al-Skeini) v. Sec'y of State for Def. [2007] UKHL 26 [45], [2008] 1 AC 153 (appeal taken from Eng.).

354. Echeverri Rodriguez v. Netherlands, App. No. 43286/98, at *8 (June 27, 2000), https://hudoc.echr.coe.int/eng?i=001-5366 (noting the use of information gathered from "foreign criminal investigations" as evidence in criminal proceedings "can raise [ECHR] issues . . . where there are reasons to assume that in this foreign investigation [ECHR] defence rights . . . have been disrespected."); *e.g.*, A.M. v. Italy, 1999-IX Eur. Ct. H.R. 45 ¶ ¶ 27–28 (ruling that the use of evidence obtained through MLA breached the ECHR); *cf.* Chinoy v. United Kingdom, App. No. 15199/89, at *7 (Sept. 4, 1991), https://hudoc.echr.coe.int/eng?i=001-964 (Commission) (reaching a contrary conclusion); *see* van Hoek & Luchtman, *supra* note 19, at 16–18. *But see* ZEEGERS, *supra* note 70, at 136 (noting uncertainties).

355. *Compare* Mapp v. Ohio, 367 U.S. 643, 650–60 (1961) (holding the exclusionary rule is "essential" for vindicating Fourth Amendment breaches), *with* R v. P [2002] 1 AC (HL) 146, 158–62 (appeal taken from Eng.) ("[A] breach of Article 8 did not require the exclusion of evidence."); *see* Robin Loof, *Obtaining, Adducing and Contesting Evidence from Abroad: A Defence Perspective on Cross-Border Evidence*, 2011 CRIM. L. REV. 40, 53; Andrew L.-T. Choo & Susan Nash, *Evidence Law in England and Wales: The Impact of the Human Rights Act 1998*, 7 INT'L J. EVIDENCE & PROOF 31, 43–48 (2003).

356. Othman v. United Kingdom, 2012-I Eur. Ct. H.R. 159 ¶¶ 263–267.

357. *See* ZANDER, *supra* note 187, §§ 8-60(9), 14-04.

358. Khan v. United Kingdom, 2000-V Eur. Ct. H.R. 279 ¶¶ 25–28, 34–40; *R v. P* [2002] 1 AC at 158–62; ZANDER, *supra* note 187, § 14-04; *e.g.*, R v. Magill [2006] NICC 29 [11] (N. Ir.).

359. *See* sources cited and discussion *supra* note 72.

requesting MLA,[360] they will equally assume the UK's own MLA requests have been properly executed overseas.[361] Questions about whether evidence was gathered in breach of foreign law must normally be litigated in that foreign state; UK courts will rarely entertain such issues.[362] In 2019, the Northern Ireland Crown Court, dealing with a "factual scenario" that it described as "almost certainly without precedent," ruled that evidence of confidential interviews obtained through MLA from the US was "tainted" and should be excluded under PACE § 78.[363] Other than this instance, however, or in judgments holding that the proposed use of evidence would breach the rule of specialty,[364] the only time UK courts have suggested MLA evidence may be inadmissible was when the foreign requested state subsequently alleged that its own laws had been breached during MLA.[365] Overall, although not as prohibitive as the US international silver platter doctrine,[366] the rule of non-inquiry leaves UK persons with significantly reduced digital privacy rights during MLA.[367]

4. Reciprocal US Requests

Where the US requests UK persons' data through MLA from the UK, the process will be similar as set out above.[368] UK persons have slightly wider scope to object to UK execution of an

---

360. *See supra* text accompanying notes 237–239.

361. *E.g.*, Torres v. HM Advocate (1998) SLT 811, 815–16 (Scot.); R v. Foxley [1995] 2 Cr. Ap. R. (CA) 523, 535 (Eng.). This is sometimes based on the foreign state being an ECHR member. *E.g.*, R (Unaenergy Grp. Holding) v. Dir. of Serious Fraud Off. [2017] EWHC (Admin) 600 [35](ii), [2017] 1 WLR 3302 (Eng.); Rea's (Winston Churchill) Application [2015] NICA (Civ) 8 [20], [2016] NI 203 (N. Ir.). *See generally* van Hoek & Luchtman, *supra* note 19, at 2–3 (explaining rationales).

362. *Unaenergy* [2017] EWHC (Admin) 600 [36]; Gov't of India v. Quattrocchi [2004] EWCA (Civ) 40 [27] (Eng.); *see Torres* 1998 SLT at 815–16. *See generally* Malabu Oil & Gas Ltd. v. Dir. of Public Prosecutions [2016] Lloyd's Rep. F.C. 108 (CC) [63] (Eng.) ("The extent to which the United Kingdom court will enquire into disputes about foreign law is limited both as a matter of principle and practicality.").

363. R v. Bell [2019] NICC 20 [37]–[38] (N. Ir.).

364. *E.g.*, Gohil v. Gohil [2012] EWCA (Civ) 1550 [39]–[41], [2013] 2 WLR 1123 (Eng.); *see supra* text accompanying note 253.

365. R v. I [2008] EWCA (Crim) 3062 [23]–[27] (Eng.).

366. *See supra* text accompanying note 264.

367. *See* sources cited and discussion *supra* note 72.

368. *See supra* text accompanying notes 192–271 (setting out the protections applicable during US requests for US persons' data during MLA).

MLA request as they can allege Article 8 breaches.[369] Article 8 is engaged through the use of the UK's compulsory powers during MLA,[370] although not necessarily during other forms of MLA.[371] The ECtHR has ruled that member states have breached Article 8 when executing MLA requests.[372] UK courts have, however, overwhelmingly held that Article 8 interferences during MLA are justified, citing the public interest in prosecuting crime and claiming CICA provides robust safeguards.[373]

At the final MLA stage, when the evidence is deployed in US criminal proceedings, UK persons will be in an even worse position than their US equivalents.[374] UK persons cannot raise the main joint venture exception to the international silver platter

---

369. *Cf. supra* text accompanying notes 240–248.

370. R (Sec'y of State for the Home Dep't) v. Crown Court at Southwark [2013] EWHC (Admin) 4366 [8], [28], [2014] 1 WLR 2529 [8] (Eng.); R (Hafner) v. Westminster Magistrates' Court [2008] EWHC (Admin) 524 [21], [2009] 1 WLR 1005 (Eng.). *See generally id.* [22] (noting Article 8 is engaged at all evidence-gathering stages) (citing Amann v. Switzerland [GC], 2000-II Eur. Ct. H.R. 245).

371. *E.g.*, R (Ismail) v. Sec'y of State for the Home Dep't [2016] UKSC 37 [38]–[43], [48], [2016] 1 WLR 2814 (appeal taken from Eng.) (holding that service of a judgment by the UK pursuant to a foreign state's MLA request did not in the circumstances "engage [the applicant's] fundamental rights.").

372. *E.g.*, Visy v. Slovakia, App. No. 70288/13, ¶¶ 37–47 (Oct. 16, 2018), http://hudoc.echr.coe.int/eng?i=001-186769; M.N. v. San Marino, App. No. 28005/12, ¶¶ 51–55, 74–85 (July 7, 2015), http://hudoc.echr.coe.int/eng?i=001-155819. The European Court of Human Rights (ECtHR) has confirmed generally that ECHR member states cannot rely solely on "the fact of executing a decision or an order given by . . . a foreign state . . . to relieve [that] Contracting State of [its own ECHR] obligations." Jaloud v. Netherlands [GC], 2014-VI Eur. Ct. H.R. 229 ¶143. The ECtHR has however also recognized that the ECHR may oblige its members to seek or provide MLA. *E.g.*, Güzelyurtlu v. Cyrpus and Turkey [GC], App. 36925/07, ¶¶ 191, 235–238 (Jan. 29, 2019), https://hudoc.echr.coe.int/eng?i=001-189781.

373. R (BSG Res. Ltd.) v. Dir. Of Serious Fraud Office [2015] EWHC (Admin) 1813 [19] (Eng.); H v. Lord Advocate [2011] HCJAC 77 [46], (2011) SCCR 1 (Scot.); *Hafner* [2008] EWHC (Admin) 524 [18]–[26]; Calder v. Her Majesty's Advocate [2006] HCJAC 62 [31], [29]–[32], (2007) JC 4 (Scot.); *see* Warner v. Verfides [2008] EWHC (Ch) 2609 [19], [2009] Bus. L.R. 500 (Eng.); *Crown Court at Southwark* [2013] EWHC (Admin) 4366 [8]. *But see* R v. Sec'y of State for the Home Dep't Ex p K.M. CO/3263/97, [1998] EWHC J0407-4, at *27 (QB, Apr. 7, 1998) (Eng.) (suggesting MLA electronic evidence searches may raise difficult questions). *See generally* Willcox and Hurford v. United Kingdom, 2013-I Eur. Ct. H.R. 1 ¶¶ 76, 94 (implicitly recognizing MLA's public interest).

374. *See supra* text accompanying notes 252–271.

doctrine,[375] given *Verdugo-Urquidez*.[376] It is doubtful that even the residual shocks the conscience exception will be theoretically available.[377] There appears to be no other US law basis for UK persons to exclude evidence: although UK persons benefit from the SCA,[378] as well as a limited data protection statute, the Privacy Act of 1974,[379] neither protection provides an exclusion remedy here.[380]

D. CLOUD Act Agreements Likely Also Enhance UK Persons' Digital Privacy Rights

CLOUD Act agreements will enhance UK persons' digital privacy rights, at least with respect to requests for stored data. This shift is not as pronounced as for US persons, because the MLA status quo for UK persons is not as rights-limiting, but it is

375. *See supra* text accompanying note 267.

376. *E.g.*, United States v. Gasperini, No. 16-CR-441 (NGG), 2017 WL 3038227, at *7 (E.D.N.Y. July 17, 2017) *aff'd*, 894 F.3d 482 (2d Cir. 2018); United States v. Barona, 56 F.3d 1087, 1093 (9th Cir. 1995).

377. *See supra* text accompanying note 269. If arising under the Fourth Amendment, this exception will be unavailable given *Verdugo-Urquidez*. Recent authority, discussed further below, suggests it would be unavailable even if arising under the Fifth Amendment. *See* Agency for Int'l Dev. v. All. for Open Soc'y Int'l, Inc., 140 S. Ct. 2082, 2086–87 (2020); *see also* text accompanying *infra* notes 519–522.

378. *See* sources cited *supra* note 338 and accompanying text.

379. Privacy Act of 1974, 5 U.S.C. § 552a (2014); *see* Judicial Redress Act, Pub. L. No. 114–126, 130 Stat. 282 (2016) (enacted) (codified in 5 U.S.C. § 552a note (2014)) [hereinafter JRA] (enabling extension of the Privacy Act's protections to third country nationals [TCPs]); Att'y Gen. Order No. 4381-2019, Judicial Redress Act of 2015; Attorney General Designations, 84 Fed. Reg. 3493 (Feb. 12, 2019) (JRA extension to UK persons). JRA extensions are intended to fulfill U.S. obligations under the Umbrella Agreement, *supra* note 251; *see* H.R. REP. NO. 114–294, at 4 (2015).

380. For the SCA, see 18 U.S.C. § 2707 (2018); *e.g.*, United States v. Clenney, 631 F.3d 658, 667 (4th Cir. 2011). For the Privacy Act, see H.R. REP. NO. 114–294, at 3–4 (2015) (noting it is "narrowly tailored"); *e.g.*, United States v. Moreno-Nevarez, No. 13-CR-0841-BEN, 2013 WL 5631017, at *6–*8 (S.D. Cal. Oct. 2, 2013).

nonetheless significant.[381] Potential downsides—particularly the UK's increased intercept powers—are, however, greater.[382]

1. The Impact and Operation of CLOUD Act Agreements for UK Persons

As in the US, requests for stored data under the US–UK Agreement begin similarly to MLA, with preparation of a request by law enforcement.[383] This first step also includes independent approval of the request by a UK court.[384] UK law enforcement may apply under COPOA for disclosure of stored data from providers operating in a country with which the UK has a "designated international co-operation agreement."[385] COPOA orders are similar to PACE production orders:[386] they may normally be without notice to an underlying target,[387] and law

381. *Compare supra* Section II.A (articulating US persons' protections during MLA), *with supra* Section II.C (similarly articulating UK persons' protections during MLA).

382. *Compare supra* Section II.B.2. (outlining downsides for US persons from CLOUD Act agreements), *with infra* Section II.D.2 (outlining downsides for UK persons from these agreements).

383. *See supra* text accompanying note 319.

384. *See* COPOA, §§ 1, 4. More detail about how the United Kingdom will issue CLOUD Act regime requests is available than for the United States' equivalent processes. This is because the United Kingdom has already enacted specific legislation, COPOA, for such requests. NICOLA NEWSOM, HOUSE OF LORDS LIBRARY, CRIME (OVERSEAS PRODUCTION ORDERS) BILL [HL]: BRIEFING FOR LORDS STAGES (July 5, 2018) (UK), https://researchbriefings.files.parliament.uk/documents/LLN-2018-0076/LLN-2018-0076.pdf; *see* https://lordslibrary.parliament.uk/research-briefings/lln-2018-0076/; *e.g.*, HC Deb (653) (2019) cols. 852, 859–60 (UK) (statement of Min. Wallace); *see also* U.K. HOME OFFICE, IMPACT ASSESSMENT: CRIME (OVERSEAS PRODUCTION ORDERS) BILL (2018) HO315, at 4–5 (U.K.) [hereinafter U.K. IMPACT ASSESSMENT] ("[COPOA] is the final element of legislative change required to enable U.K. law enforcement to take advantage of the proposed agreement."); Mills, *supra* note 323 at 624 (similar); *cf.* discussion *supra* note 290.

385. *See* COPOA, § 2. The UK says that these powers may be used to reach providers previously "beyond the reach of existing domestic court orders," accessible only through MLA. COPOA, Explanatory Notes ¶¶ 2–4. At the time of writing, the only UK-designated international co-operation agreement is the US–UK Agreement.

386. *See* COPOA, Explanatory Notes, ¶ 7; UK FACT SHEET, *supra* note 36, at 1; sources cited *supra* note 210.

387. *See* COPOA, §§ 1, 4; CPR, rr. 47.63–65; *see* Mills, *supra* note 323, at 624–25. Where "journalistic data" is sought, however, notice to the impacted journalist is normally required. *See* COPOA, § 12. *But see also* CPR, rr. 47.63(2), 47.76(3)(b).

enforcement must establish various "reasonable grounds."[388] Additionally, a new non-disclosure condition may be sought, expressly prohibiting disclosure of the application by providers to targets or, indeed, "any person."[389]

Once obtained, COPOA orders must be served by the UK's designated authority.[390] In contrast with MLA, the UK designated authority is not UKCA but is instead a separate Home Office Department, the Investigatory Powers Unit (IPU).[391] The provider will normally have up to one week to provide the data, absent objections.[392] While there are concerns with providers exercising this gatekeeping role,[393] taken together, these first two steps appear on balance to enhance UK persons' *ex ante* digital

388. CPR, rr. 47.67–68. When US service providers' data is sought, COPOA powers should be exercised consistently with the US–UK Agreement. *See* Assange v. Swedish Prosecution Authority [2012] UKSC 22, [2012] 2 AC 471 [10], [98], [112], [115], [122] (appeal taken from Eng.); *e.g.*, Pub. Prosecution Serv. v. Gallagher [2012] NIMag 2 [62] (N. Ir.).

389. COPOA, §§ 8, 13(5); CPR, r. 47.65(l); *cf.* sources cited *supra* note 216. Potential over-use of non-disclosure powers is concerning. *See* HL Deb (10 Sept. 2018) (793) cols. 188GC–189GC (UK) ("All my instincts are that somebody who is affected by an order should know about it."); Rebecca Niblock, *On Its Way: The UK-US Bilateral Data Access Agreement*, *Criminal Law Blog*, KINGSLEY NAPLEY (June 19, 2020), https://www.kingsleynapley.co.uk/insights/blogs/criminal-law-blog/on-its-way-the-uk-us-bilateral-data-access-agreement ("[T]he subject of the underlying investigation, be it an individual or a corporate, is likely to be blissfully ignorant of events because the Crown Court judge can include a non-disclosure requirement with the [overseas production order]."); *cf.* Criminal Procedure (Amendment No. 2) Rules 2019, SI 2019/1119, Explanatory Memorandum, ¶ 7.12 (Eng.) (stating notice must "be given in every case" unless a listed exception "exceptionally" applies).

390. COPOA, §§ 9(2), 14; *see supra* text accompanying notes 285–286.

391. *See* The Scotland Act 1998 (Agency Arrangements) (Specification) (Overseas Production Orders) Order 2021, SI2021/144, Explanatory Memorandum ¶ 7.4. Correspondence with the UK Home Office, on file with the author, states this designation occurred in January 2020 "through normal departmental processes rather than any formal designation document." The Investigatory Powers Unit "is responsible for the policy and legislation surrounding investigatory powers." UK HOME OFFICE, EXTRACT OF EVIDENCE SUPPLIED TO INDEPENDENT INQUIRY INTO CHILD SEXUAL ABUSE (HOM003247_24) [58], https://www.iicsa.org.uk/key-documents/16011/view/HOM003247_002_010_016-017_019-020_024_030-031_038_042-043.pdf.

392. *See* COPOA. § 5(5). This seven day period is standard for production orders. *E.g.*, R (Dir. of the Assets Recovery Agency) v. He [2004] EWHC (Admin) 3021 [8] (Eng.).

393. *See infra* text accompanying notes 468–491.

privacy rights relative to MLA. This is particularly apparent given the greater oversight of UK courts provided to UK persons under this new COPOA mechanism relative to MLA.[394]

These rights would undoubtedly be significantly enhanced if UK law enforcement and courts had to comply directly with Article 8 during these first two stages. Whether Article 8 is applicable is, however, debatable. Obtaining and/or serving a COPOA order may be extraterritorial under UK and ECHR law;[395] yet, as outlined, the ECHR applies extraterritorially only exceptionally.[396] Recent comments of the Grand Chamber of the ECtHR in *Big Brother Watch v. UK* suggest that Article 8 may nonetheless apply, at least, to requests targeting UK persons.[397] It is, however, difficult to evaluate the full impact of those statements, as the UK expressly declined to raise Article 1 extraterritoriality arguments in that dispute.[398] In any event, even if such requests are extraterritorial, one of the few recognized exceptions in which the ECHR extends extraterritorially may well be triggered.[399] The ECtHR has held that the ECHR applies when a member state exercises the "public powers" of a foreign government with its "consent, invitation, or acquiescence" through a treaty, other agreement or similar authority.[400] The

394. *Compare* text accompanying *supra* notes 322–331 (discussing the limited oversight of UK courts during MLA), *with* COPOA § 6(4)(c) (emphasizing the importance of not issuing COPOA orders in breach of data protection law).

395. *See* R (KBR, Inc.) v. Dir. of the Serious Fraud Off. [2021] UKSC 2 [26], [2021] 2 WLR 335 (appeal taken from Eng.) (treating similar requests as extraterritorial); UK FACT SHEET, *supra* note 36, at 1 (assuming extraterritoriality). *See generally* LAW COMMISSION, *supra* note 37, ¶ 16.38 (suggesting this issue is "finely balanced").

396. *See supra* text accompanying note 240. *But see also* Smith v. Ministry of Defence [2013] UKSC 41 [30], [2014] 1 AC 52 (appeal taken from Eng.) ("[T]he word 'exceptional' is there not to set an especially high threshold").

397. Big Brother Watch v. United Kingdom [GC], App. No. 58170/13, ¶ 497 (May 25, 2021), http://hudoc.echr.coe.int/eng?i=001-210077.

398. *Id.* ¶ 272.

399. *See* Al-Skeini v. United Kingdom [GC], 2011-IV Eur. Ct. H.R. 99 ¶¶ 130–42.

400. *Id.* ¶ 135; Al-Saadoon v. Sec'y of State for Defence [2016] EWCA (Civ) 811 [43]–[44], [46]–[57], [2017] 2 WLR 219 (Eng.); Galic v. Netherlands, App. No. 22617/07 ¶ 44 (ECtHR, June 9, 2007); *e.g.*, X and Y v. Switzerland, App Nos. 7289/75 & 7349/76, 57 Eur. Comm'n H.R. Dec. & Rep. 74 (1977) (applying this exception); *cf.* Tomanovic v. Foreign & Commonwealth Office [2019] EWHC (QB) 3350 [93]–[100], [2020] 4 WLR 5 (holding it was unavailable), *affirmed* [2021] EWCA (Civ) 117 [29] (Eng.); R (K) v. Sec'y of State for Defence [2016] EWCA (Civ) 1149 [27]–[28], [2017] 1 WLR 1671(Eng.) (similar).

US–UK Agreement appears to be precisely such an agreement, as it provides US consent for the UK to enforce public powers against US service providers that the US previously reserved for itself.[401] The UK would then be required to comply with the ECHR when acting under COPOA in relation to those within its territorial or extraterritorial jurisdiction, including UK persons, significantly enhancing their digital privacy rights at these first two stages.[402]

Once acquired, the data may be deployed as if it had been obtained domestically.[403] There will be no basis for applying the rule of non-inquiry, giving greater scope for UK courts to exclude evidence obtained in breach of rights.[404] Article 8 will undoubtedly extend to UK persons at this final stage.[405] As Article 8 "demands more than compliance with the relevant provisions of domestic law," its application may therefore provide additional protections.[406] At least in respect of stored data, therefore, CLOUD Act agreements appear to significantly enhance the protection given to the digital privacy rights of UK persons. Like their US counterparts, UK persons benefit from the full application of UK law at all stages, compared with the partial application of two states' laws under MLA.[407]

2. Potential Downsides

One downside UK persons face, similar to US persons, is the prospect that their data will be obtained through US requests.[408]

---

401. *See* US–UK AGREEMENT, *supra* note 4, arts. 5(5), 10(2); CRAWFORD, *supra* note 54. *See supra* text accompanying note 115. I elaborate on how the US–UK Agreement permits States to expand such "enforcement jurisdiction" over foreign service providers as a matter of international law elsewhere. Cochrane, *supra* note 114, at 181–189.

402. Assanidze v. Georgia [GC], 2004-II Eur. Ct. H.R. 155 ¶ 137; *see* Big Brother Watch v. United Kingdom [GC], App. No. 58170/13, ¶¶ 419–21 (Sept. 13, 2018), https://hudoc.echr.coe.int/eng?i=001-186048; *e.g.*, Privacy Int'l v. Sec'y of State for Foreign and Commonwealth Affairs [2016] UKIPTrib 14_85-CH [52], *rev'd on other grounds*; *see also supra* text accompanying notes 385–388.

403. *Cf. supra* text accompanying note 349.

404. *See supra* text accompanying notes 359–367.

405. *See supra* text accompanying note 350.

406. Calder v. Her Majesty's Advocate [2006] HCJAC 62 [32], (2007) JC 4 (Scot.); *see* Gallagher for Judicial Review (N. Ir.) v. Sec'y of the Home Dep't [2019] UKSC 3 [11]–[41], [2020] AC 185 (appeal taken from N. Ir.).

407. *See supra* text accompanying notes 295–303.

408. *See supra* text accompanying notes 311–314.

The US–UK Agreement imposes relatively fewer minimization requirements on the US, increasing the scope for incidental collection.[409] Targeting restrictions are severely reduced: while the UK is prohibited from targeting US persons at all times, the US may freely target UK persons whenever they set foot out of UK territory.[410] This downside does not displace the US–UK Agreement's overall rights-enhancing nature for UK persons, although there is a real possibility that the US may make significant use of this ability to target UK persons outside of UK territory.[411] If the US uses the SCA to target UK persons' data, UK persons will theoretically benefit from an enhanced "comity" test, triggered when providers fear that "disclosure would create a material risk . . . [of] violat[ing] the laws of" a CLOUD Act agreement country.[412]

The more significant potential downside arises from the enhanced UK intercept powers the US–UK Agreement practically enables.[413] The UK already claimed broad statutory intercept powers, most recently codified in the IPA, including asserting the ability to compel overseas service providers to assist with

409. *See* US–UK AGREEMENT, *supra* note 4, arts. 7(2)–7(4); HÖRNLE, *supra* note 164, at 215.

410. *See* US–UK AGREEMENT, *supra* note 4, at arts 1(12), 4(3); Jennifer Daskal & Peter Swire, *The U.K.-U.S. CLOUD Act Agreement Is Finally Here, Containing New Safeguards*, LAWFARE (Oct. 8, 2019, 2:33 PM), https://www.lawfareblog.com/uk-us-cloud-act-agreement-finally-here-containing-new-safeguards. This distinction arises from EU non-discrimination law. UK EXPLANATORY MEMORANDUM, *supra* note 77, ¶ 14; *see* Christakis, *21*, *supra* note 164, at III.1.

411. *See* Prabhu, Berrang & Dickey, *supra* note 45, at 180 (outlining US law enforcement policy of tracking and luring targets across borders); BOISTER, *supra* note 2, at 331 (detailing analogous US "evidence laundering" practices) (citing R v. Governor of Pentonville Prison, ex. p. Chinoy [1992] 1 All ER (QB) 317 (Eng.)); *see also* Rojszczak, *supra* note 116, at 8 (detailing numbers of non-resident UK nationals). The US may conceivably deploy similar techniques to encourage UK persons to step foot outside the UK, and to track them when they do, precisely to then target their data under the US–UK Agreement.

412. CLOUD Act § 103(a)–(b) (partly codified at 18 U.S.C. 2703(h) (2018)). The effectiveness of this new test remains debated. *E.g.*, Jennifer Daskal, Microsoft Ireland*, the CLOUD Act, and International Lawmaking 2.0*, 71 STAN. L. REV. 9, 11–13 (2018); Woods, *supra* note 175, at 400; *see also* Abraha, *supra* note 103, at 340 (expressing surprise that this test "does not explicitly include the interest of the target," including privacy rights, as relevant considerations).

413. *See infra* sources cited note 414.

intercepts.[414] Claiming these powers under UK law is one matter, enforcing them against US service providers is another altogether:[415] US service providers risked breaching the Wiretap Act by responding directly to foreign law enforcement intercept requests.[416] The UK therefore successfully negotiated for intercept powers within the US–UK Agreement.[417] As a consequence, once the US–UK Agreement comes into force, US service providers will be able to conduct intercepts for UK law enforcement, targeting UK persons or TCPs,[418] without fear of breaching the Wiretap Act,[419] thus practically increasing the extraterritorial scope of the UK intercept powers. Such intercept powers are undoubtedly highly intrusive.[420] Moreover, the UK's designation of the IPU, rather than UKCA, as the designated authority

414. IPA §§ 42, 43(3), 85, 97, 139. For prior claimed powers, *see* HL Deb (16 July 2014) (755) col. 603 (UK); DRIPA, § 4 (UK). *See generally* PAUL F. SCOTT, THE NATIONAL SECURITY CONSTITUTION 59–104 (2018) (outlining UK intercept powers); HL Deb (16 July 2014) (755) col. 648.

415. HL Deb (16 July 2014) (755) cols. 634–35 (UK); *see* ANDERSON, *supra* note 41, ¶ 13; HL Deb (27 June 2016) (773) col. 1416; *see also* 755 Parl Deb HL (5th ser.) (2014) col 648 (referring to "the extraterritoriality clause" in DRIPA as the UK's "attempt to persuade our United States service providers to cooperature with us").

416. Wiretap Act, 18 U.S.C. 119 §§ 2511(1), (4); *see* Jennifer Daskal, *Correcting the Record: Wiretaps, the CLOUD Act, and the US–UK Agreement*, JUST SECURITY (Oct. 31, 2019), https://www.justsecurity.org/66774/correcting-the-record-wiretaps-the-cloud-act-and-the-us-uk-agreement/ [hereinafter Daskal, *Correcting*].

417. *See* Daskal, *Correcting*, *supra* note 416; HL Deb (27 June 2016) (773) col. 1416 (UK); *e.g.*, *Hearing Before the Judiciary Subcomm. on Crime and Terrorism*, US S. 3, 5 (May 10, 2017) (written testimony of Paddy McGuinness, UK Deputy National Security Adviser), https://www.judiciary.senate.gov/imo/media/doc/05-24-17%20McGuinness%20Testimony.pdf.

418. The UK may compel US service providers' assistance with "targeted interception warrants." IPA §§ 15(1)(b), 15(3), 15(5), 41–43. Art. 4(5) of the US–UK Agreement prohibits use of "bulk interception" powers, *id.* § 136–157, and possibly so-called "thematic" warrants. *Id.* § 17(2); *see* HOME OFFICE, INTERCEPTION OF COMMUNICATIONS: CODE OF PRACTICE, March 2018, ¶¶ 5.11–5.28 (UK).

419. *See* US–UK AGREEMENT, *supra* note 4, at arts. 1(11), 5(3); CLOUD Act § 104(1)(A) (codified at 18 U.S.C. § 2511(j) (2018)).

420. Berger v. New York, 388 U.S. 41, 63 (1967); Roman Zakharov v. Russia [GC], 2015-VIII Eur. Ct. H.R. 205 ¶ 168; SCOTT, *supra* note 414, at 64. The IPA's powers are particularly concerning, given their opaqueness. *See* ANDERSON, *supra* note 41, ¶ 13.31. This opaqueness arises in part from a UK statutory bar prohibiting intercept evidence in court, IPA § 56, limiting effective judicial oversight. ANDERSON, *supra* note 41, ¶ 13.31(b).

responsible for transmitting US–UK Agreement orders provides some evidence that they intend to make frequent use of the US–UK Agreement for this precise purpose.[421] Nonetheless, addressing the overall impact of such increased intercept powers for UK persons and, potentially, TCPs here is beyond this article's scope. The IPA and analogous legislation are currently under challenge before European courts.[422] These judgments may ultimately limit the impact of these claimed powers, and thus lessen this potential downside for UK persons.[423]

E. Third Country Nationals' (TCPs') Digital Privacy Rights, Already Limited under MLA, Are Further Undermined by CLOUD Act Agreements

The digital privacy rights of TCPs are protected even less than those of US or UK persons under MLA. The two main constitutional mechanisms each State offers function differently: the Fourth Amendment is primarily limited extraterritorially by *nationality*; Article 8 is limited at all times by *territory*.[424] Their effect on TCPs, however, is the same; TCPs are always denied each instrument's protections.[425] Their position is even worse under the US–UK Agreement: TCPs' practical ability to enforce rights is further reduced and neither of the US–UK Agreement's claimed safeguards provides TCPs with genuine protections.

---

421. *See* sources cited *supra* note 391 and accompanying text; *cf.* text accompanying *supra* note 287 (noting that the US, in contrast, has appointed its MLA central authority, OIA, to serve as the designated authority under CLOUD Act agreements).

422. *E.g.* Priv. Int'l v. Sec'y of State for Foreign and Commonwealth Affairs, ELCI:EU:C:2020:790 (Oct. 6, 2020); R (Nat'l Council for Civ. Liberties) v. Sec'y of State for the Home Dep't [2019] EWHC (Admin) 2057, [2020] 1 WLR 243; *see also Legal Challenge: Investigatory Powers Act* LIBERTY, https://www.libertyhumanrights.org.uk/issue/legal-challenge-investigatory-powers-act/ (last visited June 24, 2021).

423. Whether any such limits would apply to TCPs depends on whether the basis on which they are imposed. If imposed pursuant to the ECHR, TCPs may not be protected given the limited extraterritorial application given to ECHR rights. *See supra* text accompanying note 240–247. If they are imposed as a result of EU law, such as the GDPR, then such limits will protect TCPs. *See, e.g.*, GDPR, *supra* note 149, at art. 2, recitals (2), (14) ("The protection afforded by [the GDPR] should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data.").

424. For further elaboration, see Daskal, *Un-territoriality*, *supra* note 1, at 339–40, 340 n.40; Bignami & Resta, *supra* note 242, at 375.

425. *See* discussion *infra* Section II.E.(1).

1. US–UK MLA Does Not Protect TCPs' Digital Privacy Rights

Consider, first, an MLA request from the US for the data of a TCP held by a UK service provider. Even if a TCP were aware of this request,[426] a preliminary US challenge would almost certainly fail, not least because Fourth Amendment objections would be unavailable.[427] TCPs would be treated in the same restrictive manner as the UK persons outlined above: both will be denied the protection of the Fourth Amendment.[428] While a TCP would have standing to challenge the UK's subsequent steps—evaluating and executing the request, and then transmitting the data—such applications have little chance of success.[429] Claims based on Article 8 would be prohibited because TCPs would be considered outside the UK's ECHR jurisdiction, just like US persons,[430] even if the TCPs are based in another ECHR state.[431] Most significantly, during US criminal proceedings, a TCP would likely be barred from even arguing for one of the narrow exceptions to the international silver platter doctrine.[432]

The reciprocal UK-initiated scenario is similar. TCPs would be precluded from raising ECHR grounds in the unlikely scenario where they knew about and were granted permission to judicially review a UK decision to issue a request.[433] Like the US persons discussed above, TCPs would be considered beyond the UK's ECHR jurisdiction.[434] They would have extremely limited options to contest the United States' subsequent evaluation and execution of the UK's MLA request because, just like UK persons, TCPs lack Fourth Amendment protections.[435] Finally,

426. *See supra* text accompanying notes 199, 329.

427. *See supra* text accompanying notes 201–204.

428. *See* discussion *supra* Section II.D.(4).

429. *See supra* text accompanying notes 223–239.

430. *See supra* text accompanying notes 240–248.

431. Human Rights Watch Inc. v. Sec'y of State for the Foreign & Commonwealth Off. [2016] UKIPTrib15_165-CH [55]; Marko Milanovic, *UK Investigatory Powers Tribunal Rules that Non-UK Residents Have No Right to Privacy under the ECHR*, EJIL: TALK! (May 18, 2016), https://www.ejiltalk.org/uk-investigatory-powers-tribunal-rules-that-non-uk-residents-have-no-right-to-privacy-under-the-echr/ (agreeing that distinctions as to the ECHR's applicability cannot be made on this basis).

432. *See supra* text accompanying notes 374–380.

433. *See supra* text accompanying notes 322–329.

434. *See supra* text accompanying notes 240–248; *cf.* text accompanying notes 330–331.

435. *See supra* text accompanying notes 343–346.

when facing the prospect of having to defend criminal proceedings, TCPs' ability to seek exclusion of MLA evidence, already limited,[436] will be further hampered by their apparent inability, like US persons, to rely on Article 8 claims, as well as, importantly, Article 6, which provides the standard ECHR mechanism through which evidence may be excluded.[437] Although UK courts claim § 78 of PACE "marches in step" with Article 6,[438] TCPs nonetheless have significantly reduced *ex post* digital privacy rights by being treated as outside ECHR jurisdiction by, at least, UK courts.[439] This loss is significant, but should not be overstated: the ECtHR has the final say on whether a TCP is within the UK's ECHR Article 1 jurisdiction.[440] At the very least, however, the inability of TCPs to ventilate ECHR claims before UK courts practically limits their effective redress options.[441] The prevailing UK interpretation that TCPs are beyond the UK's ECHR jurisdiction may, moreover, influence the ECtHR's own interpretation of this matter.[442] TCPs' inability to have Article 8 (or other) ECHR claims ventilated before the ECtHR is concerning in principle, as the ECtHR provides a further opportunity to seek redress and an important overarching "European supervision" role over the ECHR specifically.[443] It is also

436. *See supra* text accompanying notes 350–367.

437. *See supra* text accompanying notes 355–358.

438. *See* Abdurahman v. R [2019] EWCA (Crim) 2239 [111](d), [2020] 4 WLR 6 (Eng.); *see* R v. P [2002] 1 AC (HL) 146, 161–62 (appeal taken from Eng.).

439. *See infra* text accompanying notes 440–444.

440. *See infra* text accompanying note 510.

441. Rights can, in principle, be protected more quickly, cheaply, and robustly by domestic courts, rather than requiring recourse to an international court like the ECtHR. *See, e.g.*, HOME DEP'T, RIGHTS BROUGHT HOME: THE HUMAN RIGHTS BILL, 1997, Cm. 3782, ¶¶ 1.14, 1.17 (UK) (offering this as a justification for what became the HRA, and noting that, for applicants, "the road to Strasbourg is long and hard"). Effective domestic ventilation of rights claims is also consistent with the "principle of subsidiary" emphasized in a recent ECHR amendment urged by the UK. *See* Protocol No. 15 amending the ECHR, art. 1, June 24, 2013 C.E.T.S. 213 ("[T]he High Contracting Parties, in accordance with the principle of subsidiary, have the primary responsibility to secure the rights and freedoms defined in [the ECHR]."); *see* JOINT COMM. ON HUM. RTS., PROTOCOL 15 TO THE EUROPEAN CONVENTION ON HUMAN RIGHTS, FOURTH REPORT OF SESSION 2014–15, HL 71, §§ 2–3 (UK).

442. *See* Priv. Int'l v. United Kingdom, App. No. 46259/16, ¶¶ 42–43 (July 7, 2020), https://hudoc.echr.coe.int/eng?i=001-204588.

443. *E.g.,* Mosley v. United Kingdom, App. No. 48009/08, 53 Eur. H.R. Rep. 30, ¶ 107 (2011); *cf.* JOINT COMM. ON HUM. RTS.*, supra* note 441, § 2.6.

worrying in practice, as the ECtHR has a much greater track record of upholding Article 8 than UK courts.[444]

2. CLOUD Act Agreements Further Undermine TCPs' Digital Privacy Rights

A core change that CLOUD Act agreements seek to accomplish is to shift from regulating requests for overseas service providers' data under *parts of* both US and UK law, to regulating these requests under the *full* application of the requesting state's law only.[445] This change is on balance rights-enhancing for US and UK persons, who should receive greater Fourth Amendment and Article 8 protections, respectively.[446] It will, however, have the opposite effect for TCPs. While the US–UK Agreement specifically allows TCP targeting,[447] TCPs continue to be denied the protections of either rights instrument: *Verdugo-Urquidez* continues to apply under US law;[448] and TCPs also remain beyond the UK's ECHR jurisdiction. The analysis above imagined that the UK's ECHR jurisdiction under Article 1 may be extended into parts of US territory when the UK makes requests under the US–UK Agreement, pursuant to the public powers exception.[449] This is, however, of no help to TCPs. TCPs—persons who are neither in the UK, nor the US, but a third country altogether—would remain outside UK ECHR jurisdiction even if it were expanded into US territory.[450] Additionally, while this article has critiqued the claim that MLA provides sufficient robust rights protection, the partial application of both US and UK law

---

444. BRICE DICKSON, HUMAN RIGHTS AND THE UNITED KINGDOM SUPREME COURT 228 (2013); *see* Hughes, *supra* note 134, at 94 ("[T]he Strasbourg Court has found Article 8 ECHR violations against the U.K. on more than 70 occasions."). Law enforcement examples include, *e.g.*, Beghal v. United Kingdom, App. No. 4755/16, (Feb. 28, 2019), https://hudoc.echr.coe.int/eng?i=001-191276; Gillan & Quinton v. United Kingdom, 2010-I Eur. Ct. H.R. 223.

445. *See* sources cited *supra* note 116 and accompanying text.

446. *See* discussion *supra* Section II.B and Section II.D.

447. *See* US–UK AGREEMENT, *supra* note 4, at art. 5(10).

448. United States v. Verdugo-Urquidez, 494 U.S. 259, 265–75 (1990); *see* discussion *supra* note 172.

449. *See supra* text accompanying notes 395–402.

450. *See* Tomanovic v. Foreign & Commonwealth Office [2019] EWHC (QB) 3350 [104], [2020] 4 WLR 5 [104] ("In order for jurisdiction to arise it is the victims that must fall within the jurisdiction of the UK for the purpose of article 1 ECHR."), *affirmed* [2021] EWCA (Civ) 117 [28] (Eng.); *cf. supra* text accompanying note 402.

may well do more to protect the rights of TCPs than the equivalent CLOUD Act agreement scenarios. Under the latter, TCPs, at least in principle, have fewer rights, as the US–UK Agreement removes one of two imperfect forums through which concerns regarding their rights may be ventilated.[451] This shift is a theoretical concern for similarly impacted persons under all direct access mechanisms.[452]

There are credible concerns that the already limited protections given to the rights of TCPs will be further undermined in practice.[453] Albert Gidari has suggested that US requests may lawfully target TCPs using "any number of lesser forms of legal process"[454] outside of the SCA and Wiretap Act's protections,[455] and without even the Fourth Amendment's reasonableness requirement.[456] UK requests for stored data would at least need to comply with COPOA,[457] but this may offer fewer protections than the MLA equivalent.[458]

---

451. *See* HÖRNLE, *supra* note 164, at 215.

452. *See id.; see also supra* text accompanying note 16 (outlining other proposed direct access mechanisms).

453. *See* discussion *supra* Section II.E.1.

454. 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), https://cyberlaw.stanford.edu/blog/2019/11/more-questions-about-cloud-act-and-us-uk-agreement-can-us-direct-uk-providers-wiretap.

455. *See* discussion *supra* note 297.

456. *Cf. supra* text accompanying notes 307–310; *see also* Smith, *supra* note 53, at 125–36 (elaborating). *But see also* text accompanying note 306 (noting that art. 5(1) of the US–UK Agreement sets certain minimum requirements).

457. *See* discussion *supra* note 384. *See generally* R (Miller) v. Sec'y of State for Exiting the European Union [2017] UKSC 5 [48], [2018] AC 61 (appeals taken from Eng. and N. Ir.) (noting alternative powers "will be displaced in a field which becomes occupied by a corresponding power conferred or regulated by statute").

458. MLA requests for communications content will be evaluated in the US against a "probable cause" standard while COPOA requires only "reasonable grounds." *See* COPOA, § 4; *see* H.R. REP. NO. 114–528, at 9 (2016); *compare* Swire & Kennedy-Mayo, *supra* note 138, at 644 ("[T]he probable cause standard is different than the legal rules in other countries, and generally considered stricter"), *with* SCOTT BAKER, DAVID PERRY, & ANAND DOOBAY, A REVIEW OF THE UNITED KINGDOM'S EXTRADITION ARRANGEMENTS ¶¶ 7.40, 7.42 (2011) ("[T]here is no significant difference between the probable cause test and the reasonable [grounds] test.").

Neither of the applicable safeguards in the US–UK Agreement offer real protection for TCPs.[459] One requires a requesting state to notify "the appropriate authorities in the third country where the person is located,"[460] although not the target TCP.[461] This is vague,[462] potentially permitting notification to be delayed until after data has been obtained.[463] It provides no clear mechanism for third country objections,[464] let alone to an independent judicial body.[465] The requesting state may avoid notification where it "considers that notification would be detrimental to operational or national security, impede the conduct of an investigation, or imperil human rights."[466] Without further clarification, there is a real risk that such broad exceptions will "become the rule."[467]

The second safeguard is the service provider itself, which may "raise specific objections when it has reasonable belief that the Agreement may not properly be invoked with regard to the [o]rder."[468] These objections will initially be considered by the issuing state but may be escalated to the provider's own state,

---

459. *See* US–UK AGREEMENT, *supra* note 4, at arts. 5(10)–(12); *see also* Service Providers Letter, *supra* note 160 ("The legislation provides mechanisms to notify foreign governments when a legal request implicates their residents, and to initiate a direct legal challenge when necessary."). The other main protection in practice under CLOUD Act agreements—targeting and minimization restrictions, *see supra* text accompanying note 126—is inapplicable to TCNs. *See supra* text accompanying note 447.

460. US–UK AGREEMENT, *supra* note 4, at Art. 5(10).

461. *See* Christakis, *21*, *supra* note 164, at III.9 (arguing the absence of target notification may be the US–UK Agreement's "most important" human rights issue).

462. *Id.* at III.6; Albert Gidari, *The Big Interception Flaw in the US–UK CLOUD Act Agreement*, CTR. FOR INTERNET & SOC'Y (OCT. 18, 2019, 9:00 AM), http://cyberlaw.stanford.edu/blog/2019/10/big-interception-flaw-us-uk-cloud-act-agreement [hereinafter Gidari, *Big Interception Flaw*].

463. Gidari, *Big Interception Flaw*, *supra* note 462.

464. Abraha, *supra* note 103, at 345; Christakis, *21*, *supra* note 164, at Chart 1, cmt. 7.

465. Gidari, *Big Interception Flaw*, *supra* note 463; *cf.* Daskal & Swire, *supra* note 429.

466. US–UK AGREEMENT, *supra* note 4, at art. 5(10); *see* Abraha, *supra* note 103, at 345 ("[It] is subject to the unilateral decision of the Issuing Party."); Gidari, *Big Interception Flaw*, *supra* note 463 ("The discretion seems absolute.").

467. *See* Christakis, *21*, *supra* note 164, at III.6.

468. US–UK AGREEMENT, *supra* note 4, at art. 5(11).

which has the "ultimate veto power."[469] Providers can already object to demands for customers' data in the US and UK.[470] Their role takes on added significance here, however, as they do so in an environment in which the "layer of domestic review" applicable in MLA is absent.[471] As discussed above, a MLA requested state will review and authorize an incoming MLA data request, apply for, obtain, and execute a court order for that data, and finally transmit that data back.[472] In contrast, under CLOUD Act agreements, the provider will provide the primary protection for TCPs' rights.[473] The motivation of providers to object to demands for customers' data is, however, debated.[474] On the one hand, their interests as private companies, driven by commercial influences,[475] may well differ from the interests of targets, particularly TCPs.[476] Providers may be held in contempt for disputing requests,[477] yet receive statutory protection for

469. *Id.* at arts. 5(11)–(12); Daskal & Swire, *supra* note 410.

470. *E.g.*, *In re* Search Warrant No. 16-960-M-1 to Google, 275 F. Supp. 3d 605, 606 (E.D. Pa. 2017); R (NTL Grp. Ltd.) v. Ipswich Crown Court [2002] EWHC (Admin) 1585, [2003] QB 131. *But see supra* notes 215, 341 and accompanying text.

471. Eleni Kyriakides, *Digital Free for All Part Deux: European Commission Proposal on E-Evidence*, JUST SECURITY (May 17, 2018), https://www.justsecurity.org/56408/digital-free-part-deux-european-commission-proposal-e-evidence/; *see* Jennifer Daskal, *The Opening Salvo: The CLOUD Act, e-Evidence Proposals, and EU-US Discussions Regarding Law Enforcement Access to Data Across Borders*, *in* EU LAW IN POPULIST TIMES: CRISES AND PROSPECTS 319, 338–39 (Francesca Bignami ed., 2020) [hereinafter Daskal, *Opening Salvo*] ("[T]he elimination of assisting state review . . . eliminates a key protection for targets of investigation"); sources cited *supra* note 116.

472. *See* discussion *supra* Sections II.A(2) and II.C(2). The constraints provided by a requesting state's local law, its MLA central authority, and authorizing courts are sometimes described as "gatekeepers" of rights. *See* Cochrane, *supra* note 141, at 409 (in relation to New Zealand law).

473. *See* Abraha, *supra* note 4, at 351 ("[CLOUD Act agreements . . . give service providers quasi-judicial powers"); *supra* text accompanying notes 126–128.

474. *See infra* text accompanying notes 474–482.

475. Tosza, *supra* note 143, at 20; Woods, *supra* note 175, at 366 n.225; *see* Stefan & Fuster, *supra* note 118, at vii, 40; *see* HÖRNLE, *supra* note 164, at 215.

476. Tosza, *supra* note 143, at 18. *See generally* Daskal, *Opening Salvo*, *supra* note 471, at 339 ("The location of the service provider may be totally separate from the location of the target").

477. CPR, r. 47.68; *e.g.*, Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 829 F.3d 197, 205 (2d Cir. 2016). Additional penalties may apply under wiretap statutes. Wiretap Act, 18 U.S.C. § 2522; IPA §§ 43(7)–(8).

complying.[478] They may therefore be incentivized to cooperate[479] given the likelihood of "continuing government pressure."[480] On the other hand, there is evidence that "[c]onsumers increasingly care about privacy and security."[481] At least some providers appear to be responding to consumer demands by pushing back on law enforcement requests.[482] Regardless, providers may practically lack the capacity to meaningfully protect TCPs. Unlike the equivalent MLA review process—famously decried as slow and cumbersome[483]—providers will have "a very limited timeframe" to review requests.[484] They would need "detailed knowledge of the user" targeted on which to base an objection[485]—an unlikely state of affairs.[486] They would also require knowledge of foreign

478. For the United States, *see* CLOUD Act § 104(1) (codified at 18 U.S.C. § 2511(2)(j); SCA 18 U.S.C. §§ 2702(b)(9), 2703(e) (2018)) (together holding that no cause of action is available against service providers responding to foreign CLOUD Act agreement requests). For the United Kingdom, see IPA §§ 6, 52. For further discussion on these statutory protections, which I explain purport to "immunize service providers" from almost all US and UK law liability, see Cochrane, *supra* note 114, at 170–175.

479. *See* Stefan & Fuster, *supra* note 118, at 40.

480. Jonathan Hafetz, *The Possibilities and Limits of Corporations as Privacy Protectors in the Digital Age*, *in* SURVEILLANCE, PRIVACY AND TRANSATLANTIC RELATIONS 91, 111 (David Cole, Federico Fabbrini & Stephen Schulhofer eds., 2017); *see* Tosza, *supra* note 143, at 17–18.

481. BENJAMIN MOSKOWITZ, STEPHANIE NGUYEN, MICHAEL COHEN & GINNY FAHS, CONSUMER REPORTS AND OMIDYAR NETWORK, PRIVACY FRONT & CENTER: MEETING THE COMMERCIAL OPPORTUNITY TO SUPPORT CONSUMERS RIGHTS 64 (2020).

482. *E.g.* Martin Jetter (IBM Chairman of Europe, Middle-East and Africa), *Government Access to Data: Getting the Facts Straight*, IBM (June 2, 2021), https://www.ibm.com/policy/government-access-to-data/; *see also* Isabel Laura Ebert, The Tech Company Dilemma – Navigating Government Requests for User Data (Oct. 20, 2020) (unpublished Ph.D. dissertation, University of St. Gallen) (manuscript at 96–99), https://www.alexandria.unisg.ch/262437/1/Dis5042.pdf (discussing evidence that some "progressive" service providers have adopted a "company practice involving setting rights-respecting practice as the default" in response to law enforcement data requests).

483. *See supra* text accompanying note 75.

484. Stefan & Fuster, *supra* note 118, at 40; *see supra* text accompanying note 293.

485. Rojszczak, *supra* note 116, at 8.

486. *See* Schwartz, *supra* note 44, at 1755 ("[C]loud providers do not currently verify customer identity in any rigorous manner"); *see also infra* note 505 and accompanying text.

law.[487] The provider receiving a CLOUD Act agreement request, however, will be based in a different country than the issuing law enforcement, and may be entirely unfamiliar with the issuing State's applicable law.[488] There may well be few grounds on which to base objections in any event.[489] For example, the SCA's enhanced comity test will likely be unavailable.[490] Put simply, service providers are highly unlikely to have either "the means or the know-how to thoroughly assess" and thus dispute requests.[491]

III. WHAT SHOULD BE DONE FOR TCPS? RE-THINKING EXTRATERRITORIAL DIGITAL PRIVACY RIGHTS

A. Why and How to Protect TCPs

The primary aim of CLOUD Act agreements is to speed up extraterritorial data gathering while "protecting privacy and enhancing civil liberties."[492] They also hope to avoid the "harms of data localization" and "balkanization," referring to state policies that mandate local storage of data by providers and limit foreign access.[493] The US and UK are well-placed to set privacy-

487. Requests under CLOUD Act agreements are primarily dealt with under a requesting state's own law, yet are issued to providers operating in another jurisdiction. *See supra* text accompanying note 116.

488. Daskal, *Opening Salvo*, *supra* note 472, at 338–39; GIMELSTEIN, *supra* note 146, at 6. *See generally* Christakis, *21*, *supra* note 164, at III.3 ("[T]o have a full comprehension of the [CLOUD Act] regime one needs to be simultaneously expert in International, US and UK law and to have a profound knowledge of [particular legislation.]").

489. *See supra* text accompanying notes 429–432, 435. While the US–UK Agreement incorporates the Umbrella Agreement, US–UK AGREEMENT, *supra* note 4, at art. 9(1) (citing Umbrella Agreement, *supra* note 251), its protections do not apply to TCPs beyond Europe at all under U.S. law. *See* Umbrella Agreement, *supra* note 251, art. 4; Judicial Redress Act of 2015, Attorney General Designations, 82 Fed. Reg. 7860 (Jan. 23, 2017) (extending JRA protections to EU persons); *see also* US–UK AGREEMENT, *supra* note 4, at art. 3(4) ("The provisions of this Agreement shall not give rise to a right or remedy on the part of any private person, including to obtain, suppress or exclude any evidence, or to impede the execution of Legal Process.").

490. Abraha, *supra* note 103, at 340.

491. *See* de Busser, *Digital Unfitness*, *supra* note 65, at 172.

492. Press Release, U.S. Dep't of Justice, *supra* note 5; US–UK AGREEMENT, *supra* note 4, at pmbl., art. 2.

493. US–UK AGREEMENT, *supra* note 4, at pmbl., arts. 2(1), 2(3)(c); *see* US WHITE PAPER, *supra* note 111, at 9; Downing, *supra* note 85; HL Deb (11 Oct. 2016) (774) col. 1847 (UK).

enhancing norms for the world,[494] given the US' current global data dominance.[495] At present, however, while the US–UK Agreement achieves its first aim in part, by enhancing US and UK persons' rights,[496] it undermines TCPs' rights and thus fails to achieve this aim overall.[497] This incentivizes precisely the type of data localization policies CLOUD Act agreement members seek to avoid.

From the perspective of a CLOUD Act agreement member state, what were previously "unilateral assertions of extraterritorial jurisdiction"[498]—compelling a foreign service provider to disclose data—appear to be perfectly legitimate exercises of extraterritorial enforcement jurisdiction by consent.[499] From the perspective of a TCP state, however, the legal status of such requests remains unchanged. Significantly, TCP states have not necessarily consented to the US or UK exercising jurisdiction over their nationals' data. As Swire, Daskal, and Woods all recognize, unilateral extraterritoriality assertions by one state may encourage privacy-reducing policies, including data localization, by others.[500] TCP states *may* be incentivized to seek CLOUD Act agreements,[501] but could instead take the opposite approach of pursuing data localization with vigor and even forming "anti-clubs" in opposition to the CLOUD Act agreement model.[502]

---

494. *See also* Daskal, *Law Enforcement Access*, *supra* note 40, at 500 (arguing for the United States to adopt a greater rights-focused approach here); Amy E. Pope, *Lawlessness Breeds Lawlessness: A Case for Applying the Fourth Amendment to Extraterritorial Searches*, 65 FLA. L. REV. 1917, 1922 (2013) (suggesting that United States "teach by doing" by extending rights protections over its extraterritorial acts in an analogous context).

495. *See* Daskal, *Privacy and Security*, *supra* 37, at 1050–51; Downing, *supa* note 85; *supra* text accompanying notes 42–44. It is possible, however, that this dominance is diminishing. *See* Cochrane, *supra* note 114, manuscript at 28–39.

496. *See* discussion *supra* Sections II.B. and II.D.

497. *See* discussion *supra* Section II.E.

498. Daskal, *Law Enforcement Access*, *supra* note 40, at 477–78.

499. *See* Daskal, *Hacking*, *supra* note 116, at 695.

500. *E.g.* Swire & Kennedy-Mayo*, supra* note 138, at 663–64; Daskal, *Un-Territoriality*, *supra* note 1, at 333–34, 393; Daskal & Woods, *supra* note 87.

501. *See supra* text accompanying notes 175–176.

502. *See* Woods, *supra* note 175, at 400–01; Abraha, *Mapping Policy*, *supra* note 164, at 150. *See also* Smith, *supra* note 53, at 132 (similarly warning that, insofar as CLOUD Act agreements "authorise ongoing surveillance overseas," they may lead to "destabilized relations with foreign governments.").

To minimize the likelihood of such developments, more must be done to protect TCPs' digital privacy rights. In theory, several methods are available. Targeting TCPs could be prohibited altogether.[503] This would, however, severely undermine the CLOUD Act agreement model. Investigations for transnational crimes, like terrorism, are similar to the investigations the CLOUD Act agreements are intended to facilitate: involving nationals from multiple jurisdictions.[504] It would also be ineffective because the nationality and/or location of a target is often unknown.[505] Even if requests are permitted only after the target's nationality and location are verified—further diminishing the effectiveness of CLOUD Act agreements—TCP data would still be incidentally collected and potentially deployed in breach of their rights.[506] Alternatively, enhanced statutory protections could be legislated.[507] Such protections, however, could be surpassed by judicial constitutional developments, leaving TCPs with inferior rights.[508] Moreover, TCPs implicated by UK requests would still be without "European supervision."[509]

Instead, each state should voluntarily extend the protections of the Fourth Amendment and Article 8 to TCPs implicated by CLOUD Act agreement requests. Such voluntarily extension of rights in this manner would not subject to the same structural limitations as the alternatives above. Although the Supreme

---

503. 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.

504. *See* US–UK AGREEMENT, *supra* note 4, at pmbl.; US WHITE PAPER, *supra* note 111, at 10; UK EXPLANATORY MEMORANDUM, *supra* note 77, ¶ 1. *See generally* BOISTER, *supra* note 2, at 3–42.

505. HÖRNLE, *supra* note 164, at 215; Kerr, *supra* note 166, at 303; *see* GIMELSTEIN, *supra* note 146, at 7; Daskal, *Un-Territoriality*, *supra* note 1, at 349.

506. *See supra* sources cited note 169.

507. *E.g.*, Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L. J. 805 (2003).

508. *See, e.g.*, United States v. Alahmedalabdaloklah, No. CR-12-01263-PHX-NVW, 2017 WL 2839645, at *3 (D. Ariz. July 3, 2017) (noting defendant TCN lacked standing to allege SCA unconstitutionality); *see also* R (Quark Fishing Ltd.) v. Sec'y of State for Foreign and Commonwealth Affairs [2005] UKHL 57 [32]–[44] (Lord Nicholls), [2005] 1 AC 529 (holding, despite success, applicant was not entitled to ECHR damages because they were outside the UK's ECHR Article 1 jurisdiction).

509. *See supra* text accompanying note 443–444.

Court and ECtHR remain the "ultimate" authorities for determining the scope of these rights,[510] this extension is readily achievable: the US and UK can simply not oppose constitutional claims by TCPs in litigation,[511] Ideally, the extension would also be formally recorded by amending the US–UK Agreement, as a matter of international law, and through implementing the extension of such rights through appropriate domestic law mechanisms.[512] This extension is also consistent with the trend of caselaw in each jurisdiction, as addressed below.

B. Extending Fourth Amendment Protections

Although US courts continue to commonly apply *Verdugo-Urquidez* to deny rights to TCPs in this context,[513] an extension of Fourth Amendment rights would nonetheless be an appropriate incremental step in the context of wider Supreme Court

---

510. *See* Baker v. Carr, 369 U.S. 186, 211 (1962) (referring to the Supreme Court "as ultimate interpreter of the Constitution"); R (Priv. Int'l) v. Investigatory Powers Tribunal [2019] UKSC 22 [142], [2020] AC 491 ("[T]he ultimate arbiter of [ECHR] law is in Strasbourg rather than the courts of this country.").

511. *E.g.*, United States v. Ross, 963 F.3d 1056, 1065–66 (11th Cir. 2020); Big Brother Watch v. United Kingdom, App. No. 58170/13, ¶ 271 (Sept. 13, 2018), https://hudoc.echr.coe.int/eng?i=001-186048; *see* R (Gudanaviciene) v. Dir. of Legal Aid Casework [2014] EWCA (Civ) 1622 [168]–[169], [2015] 1 WLR 2247 (recording counsel submission that, despite ECHR Article 1 case law, "there are many cases in which the courts have reached decisions on article 8 grounds where the persons concerned are outside the jurisdiction").

512. *See* US–UK AGREEMENT, *supra* note 4, at art. 16 (contemplating amendments). While the precise form of any domestic law mechanisms would depend on US and UK law, these range from simply a published policy statement, *e.g.*, R (Begum) v. Sec'y of State for the Home Dep't [2021] UKSC 7 [21]–[22], [2021] AC 765 (appeal taken from Eng.) (referring to a UK policy to voluntarily extend certain ECHR rights abroad), through to secondary legislation or administrative rules published by the US or UK government. *See generally* United States v. Verdugo-Urquidez, 494 U.S. 259, 275 (1990) (acknowledging the United States may impose "restrictions on searches and seizures" by US agents abroad). More robustly—and more theoretically—this extension of rights could be achieved through primary legislation or, in the US' case, a Constitutional amendment.

513. Jennifer Daskal, *Transnational Seizures: The Constitution and Criminal Procedure Abroad*, *in* CONSTITUTIONALISM ACROSS BORDERS IN THE STRUGGLE AGAINST TERRORISM 191, 196–97 (Federico Fabbrini & Vicki C. Jackson eds., 2016) [hereinafter Daskal, *Transnational Seizures*]; *see supra* text accompanying note 345.

jurisprudence.[514] In 2008, the Supreme Court decided *Boumediene v. Bush*, holding that "questions of extraterritoriality turn on objective factors and practical concerns, not formalism."[515] While courts and scholars have emphasized that *Boumediene* unsettles the existing extraterritorially doctrine,[516] the Supreme Court appears to have endorsed a "functional approach" to extraterritorial rights in this judgment,[517] emphasizing certain factors.[518] Although an opinion authored by Justice Kavanaugh for the court in mid-2020 asserted that TCPs "do not possess rights under the US Constitution,"[519] his comments may be *obiter dicta.*[520] These were issued with specific regard to a

514. Hernández v. Mesa, 137 S. Ct. 2003, 2007 (2017); Boumediene v. Bush, 553 U.S. 723, 763–64 (2008). *But see* Agency for Int'l Dev. v. All. for Open Soc'y Int'l, Inc., 140 S. Ct. 2082, 2086–87 (2020); Zadvydas v. Davis, 533 U.S. 678, 693 (2001).

515. *Boumediene*, 553 U.S. at 763–64.

516. *E.g.*, Hamad v. Gates, 732 F.3d 990, 1005 (9th Cir. 2013); United States v. Wanigasinghe, 545 F.3d 595, 597 (7th Cir. 2008); Al Otro Lado, Inc., v. McAleenan, 394 F. Supp. 3d 1168, 1221 (S.D. Cal. 2019); United States v. Hayes, 99 F. Supp. 3d 409, 413–15 (S.D.N.Y. 2015); Fatma E. Marouf, *Extraterritorial Rights in Border Enforcement*, 77 WASH. & LEE. L. REV. 751, 816–17 (2020); Margaret Kopel, Comment, *Injustice at the Border: Application of the Constitution Abroad through the Conflict of Laws*, 167 U. PA. L. REV. 1241, 1250 (2019); Daskal, *Transnational Seizures*, *supra* note 513, at 196–97.

517. Daskal, *Transnational Seizures*, *supra* note 513, at 195–96. The plurality in *Verdugo-Urquidez*, delivered by Chief Justice Rehnquist, partly sought to justify limiting rights on a tortured interpretation of the Fourth Amendment phrase "the people," *Verdugo-Urquidez*, 494 U.S. at 265–66. However, the crucial fifth vote provided by Justice Kennedy expressly rejected that reasoning. *Id.* at 276 (Kennedy, J., concurring); LaFave, *supra* note 187, § 1.8(h); *see* Daskal, *Transnational Seizures*, *supra* note 513, at 202; Cole, *supra* note 11, at 371 n.16.

518. *Boumediene*. 553 U.S. at 764–6; *Verdugo-Urquidez*, 494 U.S. at 274–75; *see also Agency for Int'l Dev.*, 140 S. Ct. at 2099–100 (Breyer, J., dissenting) (synthesizing these factors as "the extent of de facto U. S. Government control (if any) over foreign territory," as well as "the nature of the constitutional protection sought, how feasible extending it would be in a given case, and the foreign citizen's status vis-à-vis the United States," and cautioning that "other pertinent circumstances . . . might arise.") (citations omitted).

519. *Agency for Int'l Dev.*, 140 S. Ct. at 2086.

520. *Id.* at 2099 (Breyer, J., dissenting) (referring to this as a "sweeping assertion [which] is neither relevant to this case nor correct on the law"). *See generally Obiter Dictum*, BLACK'S LAW DICTIONARY (11th ed. 2019) ("A judicial comment made while delivering a judicial opinion, but one that is unnecessary to the decision in the case and therefore not precedential (although it may be considered persuasive).").

foreign corporation's First Amendment rights—a very different context compared with TCPs' rights under CLOUD Act agreements—and were subject to a persuasive dissent from Justice Breyer.[521] The impact of Justice Kavanaugh's comments for the future protection of TCPs' constitutional rights therefore remains to be seen.[522]

Extending the Fourth Amendment's protections to TCPs in this context would simply require the US to provide the same *ex ante* protections—when TCPs are targeted—and the same *ex post* remedies—if and when TCPs are prosecuted in US courts—that it would for US persons.[523] This would be appropriate under the functional approach.[524] The relationship of these TCPs with the US would arise directly from the US' own requests targeting or otherwise implicating TCPs' data.[525] This would provide important protections for TCPs.[526] The "sites" over which these protections are sought—perhaps best conceived of as virtual locations comprising the data of TCPs held by foreign service providers—"in every practical sense" are "within the constant jurisdiction of the [US]" under the US–UK Agreement.[527]

---

521. *Agency for Int'l Dev.*, 140 S. Ct. at 2099–100.

522. *See Leading Case*, Agency for International Development v. Alliance for Open Society International, Inc., 140 S. Ct. 2082 (2020), 134 HARV. L. REV. 490, 494–499 (2020); Joshua J. Schroeder, *Conservative Progressivism in Immigrant Habeas Court: Why* Boumediene v. Bush *is the Baseline Constitutional Minimum*, 45 N.Y.U. REV. OF L. & SOC. CHANGE: THE HARBINGER 46, 67–71, 67 n.67 (2021); *e.g.*, Thunder Studios, Inc. v. Kazal, 13 F.4th 736, 744 (9th Cir 2021); *Al Hela v. Trump*, 972 F.3d 120, 148 (D.C. Cir. 2020); *In re* Google LLC, 337 F.R.D. 639, 649 (N.D. Cal. 2020); United States v. Guzman-Hernandez 487 F. Supp. 3d 985, 990 (E.D. Wash. 2020).

523. *See* discussion *supra* Section II.B(1).

524. *See supra* sources cited note 518 and accompanying text.

525. *See* Boumediene v. Bush, 553 U.S. 723, 766 (2008) (referring to "the citizenship and status of the detainee" vis-à-vis the United States"); *Agency for Int'l Dev.*, 140 S. Ct. at 2100 (Breyer, J., dissenting) (similarly referring to "the foreign citizen's status vis-à-vis the United States" as relevant).

526. *See Boumediene*, 553 U.S. at 766 (referring to "the procedural protections afforded to the detainees" as "far more limited, and … fall[ing] well short of the procedures and adversarial mechanisms that would eliminate the need for" Constitutional protections); *Agency for Int'l Dev.*, 140 S. Ct. at 2100 (Breyer, J., dissenting) (noting as relevant "the nature of the constitutional protection sought").

527. *Boumediene*, 553 U.S. at 766, 768; *see Agency for Int'l Dev.*, 140 S. Ct. at 2100 (Breyer, J., dissenting) (relevant factors "include the extent of *de facto* U.S. Government control (if any) over foreign territory").

This approach would also be practical.[528] It would not be resource intensive;[529] it would simply require treating TCPs similar to US persons.[530] There is no need to grapple with "differing and perhaps unascertainable" foreign law[531] because CLOUD Act agreement requests by the US will be governed primarily by US law.[532] A US warrant will not be a "dead letter" in this context.[533] It will no longer be true that "an American law enforcement officer would not be permitted under British law to waltz into a London premises and execute [a] search authorized by the American magistrate judge."[534] Rather, the CLOUD Act

528. *See Agency for Int'l Dev.*, 140 S. Ct. at 2100 (Breyer, J., dissenting) (asking "how feasible extending [the right sought] would be in a given case"); *Boumediene*, 553 U.S. at 766 (considering "practical obstacles"); United States v. Verdugo-Urquidez, 494 U.S. 259, 278 (1990) (Kennedy, J., concurring) (noting "[t]he conditions and considerations of this case [which] would make adherence to the Fourth Amendment's warrant requirement impracticable and anomalous."); *see also* Fitisemanu v. United States, 1 F.4th 862, 902 (10th Cir. 2021) (interpreting "impracticable" as setting a high bar and concluding that "[i]f it's not impracticable to implement a constitutional right in a territory, the court must do so unless it would be 'anomalous'.").

529. *Cf. Boumediene*, 553 U.S. at 766 (extraterritorial application of Constitutional rights may be appropriate even where there are "costs," including the "expenditure of funds").

530. *Cf. Verdugo-Urquidez*, 494 U.S. at 274 (suggesting that it would be overly burdensome to require US law enforcement to establish probable cause for overseas acts); *see supra* text accompanying note 523. Notably, Daskal argues where a target's nationality is unknown Fourth Amendment protections should be assumed. Daskal, *Un-Territoriality*, *supra* note 1, at 383–86; *see also* Kerr, *supra* note 166, at 308–10 (suggesting the United States should assume Fourth Amendment applicability absent a contrary "reasonable, good faith belief"). This suggests it would not be onerous to treat all TCPs as attracting Fourth Amendment protections.

531. *Cf. Verdugo-Urquidez*, 494 U.S. at 274 (claiming extending the Fourth Amendment abroad "would plunge [courts] into a sea of uncertainty as to what might be reasonable in the way of searches and seizures conducted abroad."); *id.* at 278 (Kennedy, J., concurring) (noting "the differing and perhaps unascertainable conceptions of reasonableness and privacy that prevail abroad").

532. *See* sources cited and discussion *supra* note 116.

533. *Verdugo-Urquidez*, 494 U.S. at 274; *see id.* at 278 (Kennedy, J., concurring) (referring to "[t]he absence of local judges or magistrates available to issue warrants" and "the need to cooperate with foreign officials" as meaning that warrants enforced overseas would be merely "dead letters"); *id.* at 279 (Stevens, J., concurring) (similar). *See generally Dead Letter*, BLACK'S LAW DICTIONARY (11th ed. 2019) ("A law or practice that, although not formally abolished, is no longer observed, or enforced.").

534. United States v. Vilar, No. S305–CR–621 (KMK), 2007 WL 1075041, at *52 (S.D.N.Y., Apr. 4, 2007).

agreements will allow this "waltzing" to occur, albeit virtually. Further, far from risking "deleterious consequences" for US foreign policy,[535] recognizing TCP Fourth Amendment protections will minimize potential "diplomatic and legal complications" from TCP states.[536]

C. Extending Article 8 Protections

A similar story can be told about ECtHR jurisprudence.[537] The ECtHR has adopted a "more expansive" approach to extraterritoriality in recent years.[538] This began with the 2011 judgment of its Grand Chamber, *Al-Skeini v. United Kingdom*, which held that Iraqi nationals impacted by UK operations there were within the UK's ECHR jurisdiction.[539] Subsequent cases have expanded this—all, like *Al-Skeini*, considering the extraterritorial application of the ECHR to acts carried out over overseas physical territory.[540] The ECtHR has never articulated how ECHR jurisdiction should be interpreted in the digital sphere,[541] nor has it expressly overruled its own previous narrow

---

535. *Verdugo-Urquidez*, 494 U.S. at 273–74.

536. *In re* Terrorist Bombings of U.S. Embassies in East Africa, 552 F.3d 157, 171 (2d Cir. 2008) (citing *Vilar*, WL 1075041, at *52); *see supra* text accompanying note 502.

537. *E.g.*, Georgia v. Russia (II) [GC], App. No. 38263/08, ¶¶ 113–124 (Jan. 21, 2021), https://hudoc.echr.coe.int/eng?i=001-207757; M.N. v. Belgium, App. No. 3599/18 ¶¶ 99–109 (Mar. 5, 2020), https://hudoc.echr.coe.int/fre?i=001-202468; Jaloud v. Netherlands [GC], 2014-VI Eur. Ct. H.R. 229 ¶¶ 137–53; Al-Skeini v. United Kingdom [GC], 2011-IV Eur. Ct. H.R. 99 ¶¶ 130–50; *see also* Bankovic v. United Kingdom [GC], 2001-XII Eur. Ct. H.R. 333 ¶¶ 59–61 (exemplifying the ECtHR's prior approach).

538. Milanovic, *Jurisdiction*, *supra* note 241, at 102.

539. *Al-Skeini*, 2011-IV Eur. Ct. H.R. 99 ¶¶ 130–50.

540. *See Georgia*, App. No. 38263/08, ¶¶ 114, Al-Waheed v. Ministry of Defence [2017] UKSC 2 [47], [121], [2017] AC 821 (appeals taken from Eng.); Al-Saadoon v. Sec'y of State for Defence [2016] EWCA (Civ) 811 [33], [2017] 2 WLR 219 (Eng.). *See generally* Milanovic, *Jurisdiction*, *supra* note 241, at 97 ("[The [ECtHR] is growing increasingly comfortable with applying the [ECHR] extraterritorially"), Eliza Watt, *The Role of International Human Rights Law in the Protection of Online Privacy in the Age of Surveillance*, *in* 2017 9TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT: DEFENDING THE CORE 93, 101 (H. Rõigas, R. Jakschis, L. Lindström & T. Minárk eds., 2017) (similar). Regarding the ECtHR's focus on overseas physical territory in this context, *see e.g.*, *Jaloud*, 2014-VI Eur. Ct. H.R. 229 ¶ 152; Lea Raible, *The Extraterritoriality of the ECHR: Why* Jaloud *and* Pisari *Should be Read as Game Changers*, 2 EUR. HUM. RTS. L. REV. 161 (2016).

541. *See* sources cited *supra* note 242 and accompanying text.

extraterritoriality judgments.[542] Instead, it proceeds slowly, attempting to fit new fact scenarios inside its existing extraterritoriality framework.[543] This has been criticized as generating a "patch-work" of inconsistent and confusing extraterritoriality case law.[544] UK courts have additionally adopted a historically conservative approach to Articles 1 and 8 specifically and often shown an unwillingness to expand ECHR rights beyond what the ECtHR has definitively declared generally.[545] Together, the ECtHR's 'patchwork' approach and the conservative approach of UK courts to the ECHR have enabled and led to the narrow UK interpretation to Article 8's extraterritorial reach exemplified in *Human Rights Watch* and similar cases.[546]

Extending Article 8 protections to TCPs would be consistent with the overall trend of the ECtHR's jurisprudence and its underlying principles.[547] An extension of these protections would also be eminently preferable to *Human Rights Watch*, which has

542. Samantha Besson, *The Extraterritoriality of the European Convention on Human Rights: Why Human Rights Depend on Jurisdiction and What Jurisdiction Amounts to*, 25 LEIDEN J. INT'L L. 857, 859 n.13 (2012) ("[I]t is quite remarkable that the Court decided to overrule part of its *Bankovic* precedent in *Al-Skeini*, albeit without recognizing that it was doing so").

543. *E.g.*, M.N. v. Belgium, App. No. 3599/18 ¶¶ 99–109 (Mar. 5, 2020), https://hudoc.echr.coe.int/fre?i=001-202468; *Al-Skeini*, 2011-IV Eur. Ct. H.R. ¶ 132; *see Al-Saadoon* [2016] EWCA (Civ) 811 [29]; Marko Milanovic, Al-Skeini *and* Al-Jedda *in Strasbourg*, 23 EUR. J. INT'L L. 121, 127 (2012).

544. *Al-Skeini*, 2011-IV Eur. Ct. H.R. 99 ¶ 5 (Bonello, J., concurring); Raible, *supra* note 540, at 161; *e.g.*, Milanovic, *Jurisdiction*, *supra* note 241 at 98; Wilson, *supra* note 242, at 145; Holly Huxtable, *E.T. Phone Home…They Know: The Extraterritorial Application of Human Rights Treaties in the Context of Foreign Surveillance*, 28 SEC. & HUM. RTS. 92, 102 (2017).

545. For the UK's narrow approach to Article 8, *see supra* note 444. For its approach to Article 1, *see, e.g.*, R (Al-Skeini) v. Sec'y of State for Def. [2007] UKHL 26 [60]–[83], [2008] 1 AC 153 (appeal taken from Eng.); *see also Al-Saadoon*, [2016] EWCA (Civ) 811 [70] ("[As] repeatedly stated in the House of Lords and the Supreme Court, … Article 1 should not be construed as reaching any further than the existing Strasbourg jurisprudence clearly shows it to reach."). *See generally* R (AB) v Sec'y of State for Just. [2021] UKSC 28 [57], [2021] 3 WLR 494 (reaffirming that UK courts should take a "conservative approach" to interpreting ECHR rights generally).

546. Human Rights Watch Inc. v. Sec'y of State for the Foreign & Commonwealth Off. [2016] UKIPTrib15_165-CH [56]–[61]; Wilson, *supra* note 242, at 144; *see supra* notes 243–247.

547. *See generally* Raible, *supra* note 243, at 520–24 (similarly arguing for "principled reasoning").

been extensively criticized.[548] The ECtHR has suggested that protection gaps for rights generated through narrow interpretations to Article 1 should be avoided.[549] While the recent *Big Brother Watch* Grand Chamber judgment does not directly address ECHR extraterritoriality issues,[550] it similarly stresses that the ECHR's protections should not "be rendered nugatory"

548. Wilson, *supra* note 243, at 144–46 (criticizing the judgment as "lustreless"); Helen McDermott, *Application of the International Human Rights Law Framework in Cyber Space*, *in* HUMAN RIGHTS AND 21ST CENTURY CHALLENGES: POVERTY, CONFLICT, AND THE ENVIRONMENT 190, 203–04 (Dapo Akande, Jakko Kuosmanen, Helen McDermott & Dominic Roser eds., 2020) (concluding that it is contrary to ECtHR jurisprudence and noting "[t]he logic behind the extension of obligations to extraterritorial cyber operations is obvious"); Huxtable, *supra* note 544 (opining that the judgment was wrong and indirectly criticizing it throughout); Raible, *supra* note 243 (viewing it as "unsatisfactory" and insufficiently engaging with ECtHR jurisprudence, and suggesting a more principled approach); Milanovic, *supra* note 431 (arguing that it was "fundamental mistaken"). Others, not directly critiquing, suggest the ECtHR may take a different view. Kristian P. Humble, *International Law, Surveillance and the Protection of Privacy*, 25 INT'L J. HUM. RTS. 1, 10 (2021) (referring to it as "controversial"); Cedric M.J. Ryngaert & Nico A.N.M. van Eijk, *International Cooperation by (European) Security and Intelligence Services: Reviewing the Creation of a Joint Database in Light of Data Protection Guarantees*, 9 INT'L DATA PRIV. L. 61, 67 (2019) (calling it "[a]rguably … too restrictive."); Bignami & Resta, *supra* note 242, at 377 ("It is by no means obvious, however, that the European Court will adopt the same stance"); *see also* Altwicker, *supra* note 19, at 587 (saying it "may be short-sighted" for several reasons); Watt, *supra* note 539, at 99–100 (characterizing it as "a conservative approach").

549. Issa v. Turkey, App. No. 31821/96, 41 Eur. H.R. Rep. 27, ¶ 71 (2005) ("Art[icle] 1 of the Convention cannot be interpreted so as to allow a [S]tate party to perpetrate violations of the Convention on the territory of another [S]tate, which it could not perpetrate on its own territory."); *see Al-Saadoon*, [2016] EWCA (Civ) 811 [32] (applying *Issa v. Turkey*); Wilson, *supra* note 242, at 145 (elaborating); *see also* Carter v. Russia, App. No. 20914/07, ¶ 127 (Sept. 21, 2021), https://hudoc.echr.coe.int/eng?i=001-21197 (affirming and extending the analysis in *Issa v Turkey* to extraterritorial "[t]argeted violations of the human rights of an individual").

550. *See supra* text accompanying note 398. *But see* Marko Milanovic, *The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum för Rättvisa*, EJIL: Talk! (May 26, 2021), https://www.ejiltalk.org/the-grand-normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa/ (suggesting that aspects of *Big Brother Watch* "may be a hint" that the ECtHR would recognize that TCPs may be within the ECHR jurisdiction of a state in certain surveillance scenarios).

when member states seek data from non-contracting states, including through related "direct access" methods.[551]

The ECtHR has underscored the importance of ensuring Article 8 develops alongside new technologies,[552] and emphasized that states pioneering such technologies have a "special responsibility for striking the right balance" with rights.[553] It has also treated state practice as relevant to questions of Article 1 jurisdiction.[554] The UK, for example, raised no jurisdictional objection to Article 8 claims by TCPs in two recent cases.[555] These principles suggest that, when such a case is before the ECtHR, it should shift from its previous focus on *physical* control to a greater recognition that control may be exercised entirely virtually,[556] reflecting today's digital era.[557] Overall, these factors support finding that TCPs implicated by UK acts under the US–UK Agreement are "within their jurisdiction" for the purposes of Article 1.

CONCLUSION

The rights-enhancing aims of CLOUD Act agreements should be welcomed. Much more is required, however, for these aims to be realized. The current protection gaps under the US–UK Agreement threaten to undermine rights for TCPs—i.e. most persons across the world. This encourages data localization and similar policies, which are precisely the developments that the

551. Big Brother Watch v. United Kingdom [GC], App. No. 58170/13, ¶ 497 (May 25, 2021), http://hudoc.echr.coe.int/eng?i=001-210077.

552. Szabó & Vissy v. Hungary, App. No. 37138/14, ¶¶ 53, 62, 68, 73, 89 (Jan. 12, 2016), https://hudoc.echr.coe.int/fre?i=001-160020; Roman Zakharov v. Russia [GC], 2018-VIII Eur. Ct. H.R. 205 ¶ 229.

553. S. and Marper v. United Kingdom [GC], 2008-V Eur. Ct. H.R. 167 ¶ 112.

554. Hassan v. United Kingdom [GC], 2014-VI Eur. Ct. H.R. 1, ¶¶ 100–01.

555. *Big Brother Watch* , App. No. 58170/13, ¶ 271–72; Liberty v. United Kingdom, App. No. 58243/00, 48 Eur. H.R. Rep. 1, 22 (2009); *see also* Weber v. Germany, 2006-XI Eur. Ct. H.R. 309, ¶¶ 66, 72 (declining to consider a jurisdictional objection, instead dismissing on other grounds).

556. Peter Margulies, *The NSA in the Global Perspective: Surveillance, Human Rights, and International Counterterrorism*, 82 FORDHAM L. REV. 2137, 2139 (2014); *see* Watt, *supra* note 539, at 105; *see also, e.g.*, Ryngaert & van Eijk, *supra* note 548, at 66–67 (building on the "de-territorialized" nature of transnational data exchange" to suggest a "jurisdictional test … of 'virtual control'").

557. *Big Brother Watch* [GC], App. No. 58170/13, ¶¶ 322, 341; McDermott, *supra* note 548, at 202; Wilson, *supra* note 242, at 145; Humble, *supra* note 548, at 10; Raible, *supra* note 243, at 511.

US and UK hope to counter through CLOUD Act agreements. To avoid this, the protection gaps for TCPs should be filled, ideally through incremental extensions of the Fourth Amendment and Article 8. Taking rights seriously in this way would pay dividends: it would further the aims of CLOUD Act agreements, encourage international support and, ultimately, lead to more robust investigations and prosecutions arising from data obtained through CLOUD Act agreement requests.[558]

The comparative rights-based focus of this article may inform other developing areas of cross-border data sharing, including MLA. Long-standing concerns that MLA and other cross-border mechanisms fail to adequately protect rights remain true.[559] Indeed, MLA's continued shortcomings for rights are the main basis for this article's conclusion that CLOUD Act agreements are likely a net gain for US and UK persons. In other words, these gains are merely *relative*: by shifting from the partial application of two states' laws, under MLA, to the full application of one, under the US–UK Agreement, CLOUD Act agreements simply return many of the base-line protections these persons ordinarily have in domestic proceedings.[560] The fact, however, that MLA, at least as practiced by the US and UK, still fails to adequately protect rights, should be urgently addressed.

Myriad other issues touched on in this article deserve further study. Much of this article's evaluative analysis could be described as 'threshold,' addressing the preliminary question as to why certain persons (TCPs) should be afforded rights under the main constitutional privacy mechanisms of the US and UK. This would be welcome, not least because it would increase the scope for TCPs to seek exclusion of evidence where their rights had

---

558. *See generally* Office of the U.N. High Comm'r for Hum. Rts., *Human Rights and Law Enforcement: A Trainers Guide on Human Rights for the Police*, at 16–17, U.N. Doc. HR/P/PT/5/Add.2 (2002) (critiquing claims that rights-based investigations undermine law enforcement effectiveness).

559. *See* sourced cited and discussion *supra* note 19.

560. Both the process and the protections for rights applicable to law enforcement requests under CLOUD Act agreements much more closely resemble domestic law enforcement data collection processes than does MLA. Protection gaps relative to domestic processes may, however, remain. For example, where data is requested from foreign providers under CLOUD Act agreements, such providers may be less capable of challenging these compared with their domestic counterparts. *See* text accompanying notes 483–491.

been breached in criminal proceedings.[561] The full scope and application of digital privacy rights for targets and others implicated in cross-border law enforcement data requests is, however, a rich field for future analysis. These include the issues raised at Section I.B(2) above, of which the most pressing may be the role EU data protection law plays in regulating this field.[562]

The time is apt for the US and UK to rethink their approach to CLOUD Act agreements and other direct access mechanisms. President Biden has promised a more rights-focused approach in international affairs.[563] The UK, although now departed from the EU, recently reaffirmed its commitment to human rights in its new trade agreement with the block.[564] Most recently, in a June 2021 joint statement addressing various cross-border issues, the US and UK specifically highlighted the US–UK Agreement, stressing that privacy and data protection should lie at its heart.[565] This article offers a readily implementable way for both States to progress these commitments. Doing so would not only further the rights of TCPs and the aims of direct access mechanisms like CLOUD Act agreements, but it would also provide the US and UK an opportunity to influence a rights-based approach to cross-border data sharing—an area that will only grow in significance in the years to come.

---

561. *See* discussion *supra* Section III.E(1). Other areas of incremental reform to better protect digital privacy rights in this context should also be considered. *See, e.g.*, Daskal, *Notice*, *supra* note 283, at 454–57 (arguing that the standing of service providers to vicariously assert Fourth Amendment claims on behalf of targets should be recognized); Choo & Nash, *supra* note 355, at 43–52 (arguing for a more generous approach to exclusion of evidence in the UK).

562. *See* sources cited *supra* notes 150–151 and accompanying text.

563. Joseph R. Biden, Jr., *Why America Must Lead Again: Rescuing U.S. Foreign Policy After Trump*, FOREIGN AFFAIRS (Mar./Apr. 2020), https://www.foreignaffairs.com/articles/united-states/2020-01-23/why-america-must-lead-again.

564. Trade and Cooperation Agreement Between the European Union and the European Atomic Energy Community, of the One Part, and the United Kingdom of Great Britain and Northern Ireland, of the Other Part, pmbl. 2020 O.J. (L 444) 19; *see also* UK Adequacy Decision, *supra* note 7, (153) (confirming the UK would specifically consider data protection issues arising under the US–UK Agreement).

565. JOINT STATEMENT, *supra* note 5, ¶ 4.