DIGITAL PRIVACY RIGHTS AND THE CLOUD ACT REGIME

Tim Cochrane
Balliol College, University of Oxford

ABSTRACT

This thesis considers the impact of the new international data sharing 'CLOUD Act regime' on digital privacy rights. The first bilateral agreement of the regime, between the United States and United Kingdom, will enable UK law enforcement to directly enforce UK court orders for preservation, disclosure, and interception of electronic data against US service providers and vice versa. The CLOUD Act regime responds to long-standing concerns with the main mechanism for obtaining overseas data, mutual legal assistance (MLA). The US and UK claim that it will substantively improve on MLA while "respecting privacy and enhancing civil liberties". This thesis interrogates that claim from a rights-based perspective, focusing on the primary constitutional mechanisms protecting digital privacy rights in each state, the Fourth Amendment to the US Constitution and Article 8 of the European Convention on Human Rights. Chapter 1 explains that emerging literature is divided: US commentators view the regime as neutral or rights-enhancing, while Europeans fear a significant reduction in rights. Chapter 2 details how the shift from MLA to the CLOUD Act regime will impact these rights for three affected classes: US nationals, UK nationals, and all others, ie third country nationals (TCNs). It shows that the contrasting views are each partly right and partly wrong. The CLOUD Act regime will be largely rights-enhancing for US and UK persons, but will further reduce the already limited protections provided to TCNs, due to existing interpretations of the Fourth Amendment and Article 8, which limit their application on the basis of nationality or geography, and thus exclude TCNs. Chapter 3 argues that the jurisdictional scope of these mechanisms should be reconceptualised for today's digital world to protect TCNs' digital privacy rights and therefore uphold the rights-enhancing aims of the CLOUD Act regime.

Word count: 29,987

ACKNOWLEDGEMENTS

I am grateful for the immense support provided throughout this thesis by my supervisor, Dr Oliver Butler. He has offered immeasurable guidance, without which this thesis would not have been possible. I would also like to acknowledge the very helpful comments offered by Kaiyi Xie. Finally, I am very thankful for the continued encouragement and patience shown throughout the drafting of this thesis by my partner, Anna, particularly during the last few months of 'lockdown'.

TABLE OF CONTENTS

ABSTRACT II

ACKNOWLEDGEMENTS III

TABLE OF CONTENTS IV

TABLE OF ABBREVIATIONS VI

TABLE OF CASES VII

TABLE OF STATUTES XII

TABLE OF OTHER PRIMARY LEGAL SOURCES XIII

CHAPTER 1 1

1.1 INTRODUCTION 1

1.2 THE IMPETUS FOR AND OPERATION OF THE CLOUD ACT REGIME 4

1.2.1 Criminal investigations in the digital era 4

1.2.2 Mutual legal assistance (MLA), human rights, and 'the MLAT problem' 7

1.2.3 Attempts to solve the MLAT problem 10

1.2.4 The CLOUD Act regime and digital privacy protections 13

1.3 ASSESSING THE CLOUD ACT REGIME AGAINST DIGITAL PRIVACY RIGHTS 15

1.3.1 Digital privacy rights, cross-border conduct, and extraterritoriality 15

1.3.2 Data protection and other rights 17

1.3.3 Intelligence sharing, encryption, and hacking 19

1.4 IS THE CLOUD ACT REGIME 'BUSINESS AS USUAL' OR 'A RACE TO THE BOTTOM'? 19

1.4.1 Overall reception 19

1.4.2 Perceived impact on digital privacy rights 21

1.5 CONCLUSION 24

CHAPTER 2 26

2.1 INTRODUCTION 26

2.2 MLA FAILS TO PROTECT US PERSONS' DIGITAL PRIVACY RIGHTS 26

2.2.1 Overview 26

2.2.2 Initial US MLA steps 28

2.2.3 UK execution of US MLA requests 29

2.2.4 Subsequent US use of data 33

2.2.5 Reciprocal UK requests for US persons' data 35

2.3 THE CLOUD ACT REGIME ENHANCES US PERSONS' DIGITAL PRIVACY RIGHTS 36

2.3.1 Overview 36

2.3.3 The CLOUD Act regime appear to be rights-enhancing for US persons 37

2.3.2 Implementation uncertainties do not alter this conclusion 41

2.2.3 Reciprocal UK requests raise only limited concerns 44

2.4 UK Persons' Digital Privacy Rights Are Similarly Limited Under MLA 45
2.4.1 Overview *45*
2.4.2 Initial UK MLA steps *45*
2.4.3 US execution of UK MLA requests *47*
2.4.4 Subsequent UK use of data *48*
2.4.5 Reciprocal US requests for UK persons' data *50*
2.5 The Cloud Act Regime Likely Also Enhances UK Persons' Digital Privacy Rights 51
2.5.1 Overview *51*
2.5.2 The CLOUD Act regime largely appears to be rights-enhancing for UK persons *52*
2.5.3 Increased intercept powers may significantly undermine UK persons' rights *55*
2.5.4 Reciprocal US requests for UK persons' data raise minor concerns *56*
2.6 Third Country Nationals' (TCNs') Digital Privacy Rights, Already Limited Under MLA, Are Further Undermined By the CLOUD Act Regime 57
2.6.1 Overview *57*
2.6.2 US-UK MLA does not protect TCNs' digital privacy rights *58*
2.6.3 The CLOUD Act regime further undermines TCNs' digital privacy rights *59*
2.7 Conclusion 63
CHAPTER 3 64
3.1 Introduction 64
3.2 The Protection Gaps for TCNs' Digital Privacy Rights Under the CLOUD Act Regime Are Significant 64
3.2.1 TCNs are Exposed due to these protection gaps *64*
3.2.2 These protection gaps undermine the US and UK's own aims *66*
3.2.3 Filling these gaps by developing constitutional rights is appropriate and achievable *68*
3.3 Extending Fourth Amendment Rights to TCNs Under the CLOUD Act Regime 69
3.3.1 Overview *69*
3.3.2 There is a trend towards extraterritoriality in US Constitutional law *70*
3.3.3 Recognition of TCNs' Fourth Amendment rights here is justified under both Boumediene *and* Verdugo-Urquidez *72*
3.4 Recognising the 'Virtual Jurisdiction' of Article 8 over CLOUD Act regime Requests 76
3.4.1 Overview *76*
3.4.2 There is a trend towards increased extraterritoriality of ECHR rights *76*
3.4.3 Recognition of a 'virtual jurisdiction' under Article 8 for TCNs here is justified *80*
3.5 Conclusion 82
Bibliography 83

TABLE OF ABBREVIATIONS

CICA	Crime (International Co-operation) Act 2003 (UK)
CJEU	Court of Justice of the European Union
CLOUD Act	Clarifying Lawful Overseas Use of Data Act (US)
COPOA	Crime (Overseas Production Orders) Act 2019 (UK)
DOJ	Department of Justice (US)
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EU	European Union
GDPR	General Data Protection Regulation (EU)
HRA	Human Rights Act 1998 (UK)
IPA	Investigatory Powers Act 2016 (UK)
MLA	Mutual Legal Assistance
MLAT	Mutual Legal Assistance Treaty
OIA	Office of International Affairs (US)
PACE	Police and Criminal Evidence Act 1984 (UK)
SCA	Stored Communications Act (US)
TCN	Third Country National
UKCA	United Kingdom Central Authority
US-UK MLAT	Mutual Legal Assistance Treaty Between the United States of America and United Kingdom

TABLE OF CASES

International

Court of Justice of the European Union

Tele2 SSverige AB v Post-och telestyrelsen (C-203/15) [2017] QB 771 (CJEU)..... 18, 56
Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd (CJEU, 16 July 2020) 18

European Court of Human Rights

Al-Skeini v United Kingdom [2011] 53 EHRR 18 (GC)..... *passim*
Bankovic v UK (2007) 44 EHRR SE5..... 54, 66, 76
Beghal v UK (2019) 69 EHRR 28 59
Big Brother Watch v United Kingdom App no 58710/13 (ECtHR, 13 September 2018). ..... *passim*
Chinoy v UK App no 15199/89 (Commission Decision, 4 September 1991) 49
Echeverri Rodriguez v Netherlands App no 43286/98 (ECtHR, 27 June 2000)..... 49, 54
El-Masri v Macedonia (2013) 57 EHRR 25 (GC) 17
Gillan and Quinton v UK (2010) 50 EHRR 45..... 59
Halford v United Kingdom (1997) 24 EHRR 523 54
Issa v Turkey (2005) 41 EHHR 27..... 81
Khan v United Kingdom (2001) 31 EHRR 45..... 49
Liberty v United Kingdom (2009) 48 EHRR 1..... 77
MN v San Marino (2016) 62 EHRR 19 50
Mosley v United Kingdom (2011) 53 EHRR 1011..... 59
Othman v United Kingdom (2012) 55 EHRR 1..... 49
Soering v UK (1988) 11 EHRR 439 8
Szabo and Vissy v Hungary (2016) 63 EHRR 3..... 5
Visy v Slovakia App no 70288/13 (ECtHR, 16 October 2018)..... 50
Weber v Germany (2008) 46 EHRR SE5 77
Zakharov v Russia (2016) 63 EHRR 17 (GC) 16, 55, 81

Other International Authorities

Case of the SS Lotus (France v Turkey) (1927) PCIJ Rep Series A No 10..... 6
Corfu Channel Case (UK v Albania) (Merits) [1949] ICJ Rep 4..... 6

Domestic

United Kingdom

Abacha v Secretary of State for the Home Dept (No 1) [2001] EWHC Admin 424..... 30, 31
Abacha v Secretary of State for the Home Dept (No 2) [2001] EWHC Admin 787..... 29, 30, 31, 32
Akarcay v Chief Constable of the West Yorkshire Police [2017] EWHC 159 (Admin)..... *passim*
Al-Saadoon v Secretary of State for Defence [2015] EWHC 715 (Admin), [2016] EWCA Civ 811 65, 78, 79, 81
Amalgamated Metal Trading Ltd v City of London Police Financial Investigation Unit [2003] EWHC 703 (Comm), [2003] 1 WLR 2711..... 46
Assange v Swedish Prosecution Authority [2012] UKSC 22, [2012] 2 AC 471..... 52
Associated Provincial Picture Houses Ltd v Wednesbury Corp [1948] 1 KB 223 (EWCA) 31
Aston Cantlow and Wilmcote with Billesley Parochial Church Council v Wallbank [2003] UKHL 37, [2004] 1 AC 546..... 45
Attorney General v De Keyser's Royal Hotel [1920] AC 508 (HOL)..... 63
British Sky Broadcasting Ltd v Central Criminal Court [2014] UKSC 17, [2014] AC 885 30
BSG Resources Ltd v Director of Serious Fraud Office [2015] EWHC 1813 (Admin)..... 31, 50
C v Chief Constable of the Police Service of Scotland [2019] CSOH 48, [2019] SLT 875..... 15, 32
Calder v Frame [2006] HCJAC 62, [2007] JC 4..... 32, 50, 54

Chinoy v Governor of Pentonville Prison [1992] 1 All ER 317 (QB) 57
Director of the Assets Recovery Agency v He [2004] EWHC 3021 (Admin) 53
El Gizouli v Secretary of State for the Home Department [2020] UKSC 10, [2020] 2 WLR 857 ..... *passim*
Energy Financing Team Ltd v Bow Street Magistrates' Court [2005] EWHC 1626 (Admin), [2006] 1 WLR 1316 ..... 29, 30, 31
Fawwaz v Secretary of State for the Home Dept [2015] EWHC 166 (Admin) 31, 32
Fininvest SpA v Secretary of State for the Home Dept [1997] 1 WLR 743 (QB) 30, 31, 46
Foxley, R v, [1995] 2 Cr Ap R 523 (CA) 46, 49
Gohil v Gohil [2012] EWCA Civ 1550, [2013] 2 WLR 1123 48
Gross v Southwark Crown Court (Queen's Bench, 24 July 1998) 30, 31
H v Lord Advocate [2011] HCJAC 77, [2011 SCL 978 50
Hafeez v Southwark Crown Court [2018] EWHC 954 (Admin) 29
Hafner v Home Secretary [2006] EWHC 1259 (Admin), [2007] 1 WLR 950 ..... 29, 50
Hallam v Secretary of State for Justice [2019] UKSC 2, [2020] AC 279 16
Human Rights Watch Inc v Secretary of State for the Foreign and Commonwealth Office [2016] UKIPTrib15_165-ch ..... *passim*
Iqbai, R v, [2002] EWCA Crim 2714 48
Jimenez v The First Tier Tribunal (Tax Chamber) [2019] EWCA Civ 51, [2019] 1 WLR 2956 12
JP Morgan Chase Bank National Association v Director of the Serious Fraud Office [2012] EWHC 1674 (Admin), [2012] Lloyd's Rep FC 655 ..... 29, 30, 31, 32
KBR Inc v Director of the Serious Fraud Office [2018] EWHC 2368 (Admin), [2019] QB 675 12
Malabu Oil and Gas Ltd v Director of Public Prosecutions (Crown Court, 15 December 2015) 31, 49
McIntrye, Re [2018] NIQB 79 46
Miller v Secretary of State for Exiting the European Union [2017] UKSC 5, [2018] AC 61 63
National Council for Civil Liberties v Secretary of State for the Home Dept [2019] EWHC 2057 (Admin), [2019] 1 WLR 243 56
NTL Group Ltd v Ipswich Crown Court [2002] EWHC 1585 (Admin), [2003] QB 13 30
Okafor, R v (1994) 99 Cr App R 97 (EWCA) 59
Omega Group Holding Ltd v Kozeny EWCA Civ 798, [2005] 1 WLR 104 ..... 31, 32
Propend Finance Property ltd v Central Criminal Court [1996] 2 Cr App R 26 (QB) 30, 31
Quattrocchi, Re, [2004] EWCA Civ 40 49
R v I [2008] EWCA Crim 3062 49
R v P [2002] 1 AC 146 (HOL) 49, 55, 59
Rea's (Winston Churchill) Application [2015] NICA 8, [2016] NI 203 ..... 46, 49
Redmond, R v, [2006] EWCA Crim 1744, [2009] 1 Cr App R 25 45
River East Supplies Ltd v Crown Court at Nottingham [2017] EWHC 1942 (Admin), [2017] 4 WLR 135 . 30, 31
Sandiford v Secretary of State for Foreign and Commonwealth Affairs [2014] UKSC 44, [2014] 1 WLR 2697 ..... 32, 66, 80
Secretary of State for the Home Dept v Crown Court at Southwark [2013] EWHC 4366 (Admin), [2014] 1 WLR 2529 ..... 30, 50
Smith v Ministry of Defence [2013] UKSC 41, [2014] AC 52 65
Sorsky Defries v Southwark Crown Court (Queen's Bench, 6 July 1995) 30, 31
Superior Import / Export Ltd v Commissioners for HMRC [2017] EWHC 3172 (Admin) 31
Sutherland v Her Majesty's Advocate (Scotland) [2020] UKSC 32 59
Terra Services Ltd v National Crime Agency [2019] EWHC 3165 (Admin) 8
Terra Services Ltd v National Crime Agency [2020] EWHC 1640 (Admin) 29, 30, 31
Tomanovic v Foreign and Commonwealth Office [2019] EWHC 3350 (QB), [2020] 4 WLR 5 54
Torres v HM Advocate 1998 SLT 811 (HCJ) 49
Ullah v Special Adjudicator [2004] UKHL 26, [2004] 2 AC 323 16
Unaenergy Group Holding) v SFO [2017] EWHC 600 (Admin), [2017] 1 WLR 3302 ..... 46, 48, 49
Van der Pijl v Crown Court at Kingston [2012] EWHC 3745 (Admin), [2013] 1 WLR 2706 31
Van Der Pijl v Secretary of State for the Home Dept [2014] EWHC 281 (Admin), [2014] Lloyd's Rep 362 ... 30, 31
Warner v Verfides [2008] EWHC 2609 (Ch), [2009] Bus LR 500 50
XYZ v HM Revenue & Customs [2012] EWHC 1645 48
Zagorski v Secretary of State for Business, Innovation and Skills [2010] EWHC 3110, [2011] HRLR 6 ... 32, 66, 80
Zardari v Secretary of State for the Home Dept (No 2) (Queen's Bench, 9 April 2001) 31, 32
Zardari v Secretary of State for the Home Dept (Queen's Bench, 11 March 1998) 32
ZXC v Bloomberg [2020] EWCA Civ 611 28

United States of America

$734,578.82 in US Currency, United States v, 286 F3d 641 (3d Cir 2002) 29
Adler, United States v, 605 F Supp 2d 829 (WD Tex 2009) 34
Agency for International Development v Alliance for Open Society International Inc 591 US __, 140 SCt 2082 (2020) ..... *passim*
Ai Otro Lado Inc v McAleenan 394 F Supp 3d 1168 (SD Cal 2019) 71
Ali v Trump 959 F3d 364 (DCC 2020) 71
Ali, United States v, 71 MJ 256 (CAAF 2012) 71
Berger v State of New York 388 US 41 (1967) 27, 55
Best v United States 184 F2d 131 (1st Cir 1950) 40
Bivens v Six Unknown Named Agents of Federal Bureau of Narcotics 403 US 388 (1971) 27
Boumediene v Bush 553 US 723 (2008) ..... *passim*
Cano-Flores, United States v, 796 F3d 83 (DC Cir 2015) 42
Caro, United States v, No CR 12-964-DMG, 2015 WL 13358324 (CD Cal 2 December 2015) 42
Carpenter v US 585 US __, 138 SCt 2206 (2018) 15, 33, 35, 68
City of Ontario v Quon 560 US 746 (2010) 35
Clenney, United States v, 631 F3d 658 (4th Cir 2011) 43
Conroy, United States v, 589 F2d 1258 (5th Cir 1979) 65
Cosme, United States v, No 1-cr-394-WQH, 2011 WL 3740337 (SD Cal 2011) 42
Dahda v United States 584 US__, 138 SCt 1491 (2018) 42, 55
Defreitas, United States v, 701 F Supp 2d 297 (EDNY 2010) 34, 75
Dept of Homeland Security v Thuraissigiam 591 US __, 140 S Ct 1959 (2020) 72
Dolours Price, In re Request from the United Kingdom to the Treaty Between the Government of the United States and the Government of the United Kingdom on Mutual Assistance in Criminal Matters in the Matter of, 718 F3d 13 (1st Cir 2013) 35
Dolours Price, In re Request from United Kingdom Pursuant to Treaty Between Government of United States & Government of United Kingdom on Mutual Assistance in Criminal Matters in the Matter of, 685 F3d 1 (1st Cir 2012) 29, 35
Elkins v United States 364 US 206 (1960) 27, 40
Emmanuel, United States v, 565 F3d 1324 (11th Cir 2009) 34, 48, 65
Evtimov, United States v, No 14 CR 131–4, 2016 WL 1181828 (ND Ill, 28 March 2016) 34
Fantin, United States v, 130 F Supp 2d 385 (WDNY 2000). 51, 68
Fernandez-Caro, United States v, 677 F Supp 893 (SD Tex 1987) 40
Gasperini, United States v, 894 F3d 482 (2d Cir 2018) 51
Getto, United States v, 729 F3d 221 (2d Cir 2013) 34, 40
Gorshkov, United States v, No CR00-550C, 2001 WL 1024026 (WD Wash 23 May 2001) 43, 65
Grady v North Carolina 575 US 306 (2015) 33
Grubbs, United States v, 547 US 90 (2006). 27
Grynberg v United States Department of Justice 302 F Supp 3d 532 (SDNY 2018) 28
Hamad v Gates 732 F3d 990 (9th Cir 2013) 71
Hasbajrami, United States v, 945 F3d 641 (2d Cir 2019) 42, 44
Hayes, United States v, 99 F Supp 3d 409 (SDNY 2015) 71
Hedges v Obama 724 F3d 170 (2d Cir 2013) 71
Hernández v Mesa 589 US __, 140 S Ct 735 (2020) 71
Hernández v Mesa 582 US __, 137 S Ct 2003 (2017). 71, 74
Hernández v United States 757 F3d 249 (5th Cir 2014) 71
Herring v United States 555 US 135 (2009) 33, 34
Ibrahim v Dept of Homeland Sec 669 F3d 983 (9th Cir 2012) 48
Illinois v Gates 462 US 213 (1983) 33
In re United States 665 F Supp 2d 1210 (D Or 2009) 36
In re United States for an Order Pursuant to 18 USC § 2703(D) Misc Action No 17–2682 (BAH), 2018 WL 1521772 (DDC 8 March 2018) 36
Information Associated With Email Account (Warrant), United States v, Crim Act No 19MJ2012, 2020 WL 1499264 (ED PA 27 March 2020) 36, 53
Jackson, United States v, 849 F3d 540 (3d Cir 2017) 42
Janis, United States v, 428 US 433 (1976) 34
Jones, United States v, 565 US 400 (2012) 15

Kentucky v King 563 US 452 (2011) 33
Killen, United States v, 729 Fed Appx 703 (11th Cir 2018) 37
Kyllo v United States 533 US 27 (2001) 15, 33
Lee, United States v, 723 F3d 134 (2d Cir 2013) 34
Leon, United States v, 468 US 897 (1984) 33
Loera, United States v, 333 F Supp 3d 172 (EDNY 2018) 65
Lugo Morales, United States v, No 4:17-CR-203-ALM-KPJ, 2019 WL 1561901 (ED Tex 21 March 2019) 43
Mapp v Ohio 367 US 643 (1961) 33, 34, 49
Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp 829 F3d 197 (2nd Cir 2016) 12, 42
McLellan, United States v, 949 F3d 442 (1st Cir 2020). 29, 35
Microsoft Corp v United States Dept of Justice 233 F Supp 3d 887 (WD Wash 2017) 36
Microsoft Corp, United States v, 138 S Ct 1186 (2018) 12, 13
Microsoft Corp, United States v, 138 S Ct 356 (2017) 12
Minava, United States v, No CV 17-359 (KM), 2019 WL 1615549 (DNJ 16 April 2019) 37
Mitro, United States v, 880 F2d 1480 (1989) 40
Odoni, United States v, 782 F3d 1226 (11th Cir 2015) 34
Olaniyi, United States v, 796 Fed Appx 601 (11th Cir 2019) 71
Omar, United States v, Crim No 09–242 (MJD/FLN), 2012 WL 2277821 (D Minn, 18 June 2012) 34, 37, 48
Padilla, United States v, 508 US 77 (1993) 36
Palmat International Inc v Holder No 12-20229-CIV, 2013 WL 594695 (SD Florida, 13 February 2013) 35
Peterson, United States v, 812 F2d 486 (1987) 40, 42
Premises Located at 840 140th Ave NE Bellevue Wash, In re, 634 F3d 557 (9th Cir 2011) 29, 35, 47
Rakas v Illinois 439 US 128 (1978) 36
Reid v Covert 354 US 1 (1957) 38, 40, 65
Republic of Turkey for an Order Directing Discovery from Hamit Çiçeek Pursuant to 28 USC § 1782, In re Ex parte Petition of the, No 2:19-CIV-20107-ES-SCM, 2020 WL 2539232 (DNJ 18 May 2020) 36
Riley v California 573 US 373 (2014) 5, 15
Rodriguez, United States v, 968 F2d 130 (2d Cir 1992) 42
Rodriguez-Serna, United States v, No 18CR3739 WQH, 2019 WL 4214389 (SD Cal 5 September 2019) 42
Rojas, United States v, 812 F3d 382 (5th Cir 2016) 48
Rommy, United States v, 506 F3d 108 (2d Cir 2007) 33, 43
Ross, United States v, 963 F3d 1056 (11th Cir 2020) 69
Scully, United States v, 108 F Supp 3d 59 (EDNY 2015) 35
Search of Records, Info, & Data Associated with 14 Email Addresses Controlled by Google LLC, In re, 438 FSupp3d 771 (ED Mich 2020) 36
Search Warrant Issued to Google Inc, In re, 264 F Supp 3d 1268 (ND Al 2017) 42
Search Warrant to Google Inc, In re, Mag No 16-4116, 2017 WL 2985391 (DNJ, 10 July 2017) 42
Segura v United States 468 US 796 (1984) 34
Skinner v Railway Labor Executives Assn 489 US 602 (1989) 17
Steiger, United States v, 318 F3d 1039 (11th Cr 2003) 43
Stokes, United States v, 726 F3d 880 (7th Cir 2013) ..... *passim*
Stonehill, United States v, 274 F Supp 420 (SD Cal 1966) 34
Strieff, United States v, 579 US __, 136 SCt 2056 (2016) 33, 36
Suzlon Energy Ltd v Microsoft Corp 671 F3d 726 (9th Cir 2011) 47
Terrorist Bombings of US Embassies in East Africa, In re, 552 F3d 157 (2d Cir 2008) ..... *passim*
Toft, In re, 453 BR 186 (Bankr SDNY 2011) 47
United Kingdom v United States 238 F3d 1312 (11th Cir 2001) 29
Vega, United States v, 826 F3d 514 (DC Cir 2016) 43
Verdugo-Urquidez, United States v, 494 US 259 (1990) ..... *passim*
Vilar, United States v, Case No S3 05–CR–621 (KMK), 2007 WL 1075041 (SDNY 4 April 2007) 34, 74, 75
Wanigasinghe, United States v, 545 F3d 595 (7th Cir 2008) 71
Warshak, United States v, 631 F3d 266 (6th Cir 2010) 33, 68
Water Splash Inc v Menon 581 US __, 137 S Ct 1504 (2017) 38
Weeks v United States 232 US 383 (1914) 27, 33
Wilson v Girard 354 US 524 (1957) 38
Wilson, United States v, 322 F3d 353 (5th Cir 2003) 29
Wong Sun v United States 371 US 471 (1963) 34
Zadvydas v Davis 533 US 678 (2001) 71
Zakharov, United States v, 468 F3d 1171 (9th Cir 2006) 48

Zschernig v Miller 389 US 429 (1968) 29

Other Jurisdictions

Alsford, v R, [2017] NZSC 42, [2017] 1 NZLR 710 17
Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services [2019] ZAGPPHC 384, 2020 (1) SA 90 (GP) 15
Cox, R v, (2004) 21 CRNZ 1 (NZCA) 17
Dotcom v Attorney-General [2014] NZSC 199, [2015] 1 NZLR 745 ..... 15, 17
Marakah, R v, 2017 SCC 59, [2017] 2 SCR 608 15

TABLE OF STATUTES

United Kingdom

Statutes

Crime (International Co-operation) Act 2003 ..... *passim*
Crime Overseas Production Orders Act 2019 ..... *passim*
Criminal Justice Act 1987 52
Data Retention and Investigatory Powers Act 2014 55
Human Rights Act 1998 ..... 2, 16, 45
Investigatory Powers Act 2016 ..... *passim*
Police and Criminal Evidence Act 1984 ..... *passim*

Related instruments

Crime (International Co-operation) Act 2003 (Designation of Prosecuting Authorities) Order 2004 45
Criminal Procedure (Amendment No 2) Rules 2019 53
Criminal Procedure Rules 2015 ..... 52, 53
The Overseas Production Orders and Requests for Interception (Designation of Agreement) Regulations 2020 ..... 37, 38, 52, 55

United States

Statutes

Assistance to foreign and international tribunals and to litigants before such tribunals, 28 USC § 1782 36
Clarifying Lawful Overseas Use of Data Act (CLOUD Act), passed as part of the Consolidated Appropriations Act 2018, Pub L No 115–141, 132 Stat 348 ..... *passim*
Foreign Evidence Efficiency Act, 18 USC § 3512 36
Stored Wire and Electronic Communications and Transactional Records Access (Stored Communications Act), 18 USC §§ 2701–2713 ..... *passim*
US Constitution ..... *passim*
Wire and Electronic Communications Interception and Interception of Oral Communications (Wiretap Act), 18 USC § 2510–2523 ..... *passim*

Related instruments

Judicial Redress Act of 2015 - Attorney General Designations 82 Fed Reg 7860 (23 January 2017) 62
Judicial Redress Act of 2015 - Attorney General Designations 84 Fed Reg 3493 (12 February 2019) 62

TABLE OF OTHER PRIMARY LEGAL SOURCES

International Agreements

Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences [2016] OJ L 336/3 (US-EU Umbrella Agreement) 61

Charter of Fundamental Rights of the European Union [2012] OJ C326/02 18

Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) ..... *passim*

Convention on Cybercrime (2001) ETS 185 11

International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 3

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1 18

Bilateral Agreements

Foreign and Commonwealth Office, 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 (CP 178, 3 October 2019) ..... *passim*

Treaty between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on mutual legal assistance in criminal matters (signed 4 January 1994, entered into force 6 December 1996) 1967 UNTS 101 (as updated pursuant to various European Union measures) ..... *passim*

CHAPTER 1

1.1 Introduction

The United States and United Kingdom will soon implement the first bilateral agreement of the 'CLOUD Act regime'.[1] The CLOUD Act regime—named after its enabling US legislation, the Clarifying Lawful Overseas Use of Data Act 2018 (**CLOUD Act**)[2]—seeks to provide a quicker alternative for law enforcement to access digital evidence from overseas service providers for criminal investigations, particularly communications content.[3] It enables US and UK law enforcement to directly enforce their own court orders for the preservation, interception, and disclosure of electronic data in the other jurisdiction,[4] thus bypassing the main existing method for obtaining such data, mutual legal assistance (**MLA**).[5] Announcing their bilateral agreement, the US and UK claimed that it would improve considerably on MLA, 'while protecting privacy and enhancing civil liberties'.[6] This thesis interrogates that claim, evaluating the impact of the CLOUD Act regime on rights to privacy people enjoy over electronic data— referred to throughout this thesis as 'digital privacy rights'. It argues that the impact of this regime on these rights will be more

[1] Foreign and Commonwealth Office [**FCO**], *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* (CP 178, 3 October 2019) [**US-UK Agreement**]; Paul Greaves and Peter Swire, 'New Developments for the U.K. and Australian Executive Agreements with the U.S. Under the CLOUD Act' (*Cross-Border Data Forum*, 19 July 2020) <www.crossborderdataforum.org/new-developments-for-the-u-k-and-australian-executive-agreements-with-the-u-s-under-the-cloud-act-2/> accessed 31 July 2020.

[2] Clarifying Lawful Overseas Use of Data Act [**CLOUD Act**], passed as part of the Consolidated Appropriations Act 2018 Pub L No 115–141, 132 Stat 348 (2018).

[3] 'Service provider' includes any private entity providing 'to the public the ability to communicate, or to process or store computer data' or processing data on behalf of such a company and thus captures Google, Facebook, Apple, Dropbox, and others. See US-UK Agreement (n 1) art 1(7).

[4] Stephen P Mulligan, *Cross-Border Data Sharing Under the CLOUD Act* (Congressional Research Service, 7–500, 23 April 2018) 19–20.

[5] ibid 12–14. See generally Neil Boister, *Introduction to Transnational Criminal Law* (2nd edn, OUP 2018) ch 18.

[6] US Department of Justice [**DOJ**], 'U.S. and UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online' (3 October 2019) <www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists> accessed 31 July 2020.

nuanced than currently acknowledged, either by these states or existing literature, and that a more sophisticated understanding of how rights extend beyond nationality and borders in this context is therefore warranted.

This thesis provides the first in-depth assessment of the impact of the CLOUD Act regime on constitutional rights,[7] as well as the first detailed consideration of how it will operate in practice in both the US and UK. It focuses on digital privacy rights protected by the Fourth Amendment to the US Constitution and Article 8 of the European Convention on Human Rights (**ECHR**).[8] It compares the extent to which persons implicated by US and UK criminal investigations have effective digital privacy rights in practice under MLA when their data is sought from overseas with the position they will be in when their data is obtained under the CLOUD Act regime. This analysis draws on the existing literature critiquing the extent to which human rights are protected during MLA.[9] Building on this, it explains that, while the regime will likely be an overall improvement for the digital privacy rights of most US and UK persons, it risks further undermining the already very limited digital privacy rights these states afford to third country nationals (**TCNs**), leaving these to be protected (if at all) primarily by service providers. This consequence arises

[7] See also Peter Swire and Justin Hemmings, 'Overcoming Constitutional Objections to the CLOUD Act' (*American Constitution Society*, Issue Brief, February 2020).

[8] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) [**ECHR**]. This is given direct effect in the UK through the Human Rights Act 1998 [**HRA**].

[9] See eg C Gane and 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' (1994) 4 Eur J Crime, Crim L & Crim Just 98; Robert J Currie, 'Human Rights and International Legal Assistance: Resolving the Tension' (2000) 11 Crim L Forum 143; Aukje AH van Hoek & Michiel JJP Luchtman, 'Transnational cooperation in criminal matters and the safeguarding of human rights' (2005) 1(2) Utrecht L Rev 1; Robert J Currie, 'The protection of human rights in the suppression of transnational crime' in Neil Boister and Robert J Currie, *Routledge handbook of transnational criminal law* (Routledge, Taylor and Francis Group 2015); Maria Laura Ferioli, 'Safeguarding defendants' rights in transnational and international cooperation' in Harmen van der Wilt and Christophe Paulussen (eds), *Legal Responses to Transnational and International Crimes: Towards an Integrative Approach* (Edward Elgar 2017); Tilmann Altwicker, 'Transnationalizing Rights: International Human Rights Law in Cross-Border Contexts' (2018) 29 EJIL 581.

from long-standing judicial interpretations limiting Fourth Amendment and Article 8 protections on the basis of nationality and geography, respectively.

Underlying this thesis is an assumption that human rights, including those within constitutional mechanisms such as the ECHR and US Constitution, should be given universal effect insofar as possible. While it is beyond the scope of this thesis to defend universality, it has strong normative justifications.[10] It is also 'the driving force' behind various international human rights treaties to which the US and UK are party.[11] However, under their existing constitutional mechanisms as currently interpreted, the US and UK are primarily obligated to protect the rights of their own nationals only. At the same time, however, the acts of these states increasingly impact the digital privacy rights of TCNs through extraterritorial mechanisms like the CLOUD Act regime. These impacts were felt under MLA and are exacerbated by this new regime. As the regime functions through the laws of its members,[12] its rights-enhancing aim is undermined by the way their constitutional mechanisms protecting digital privacy rights are currently interpreted. This thesis argues for each state to adopt a more sophisticated understanding of how these rights extend extraterritorially, taking into account the 'un-territorial' nature of data.[13] It suggests that this understanding would impose positive obligations on the US and UK to protect digital privacy rights of all persons impacted by CLOUD Act regime requests, regardless of nationality or location.

---

[10] David Cole, 'Are Foreigners Entitled to the Same Constitutional Rights As Citizens?' (2003) 25 T Jefferson L Rev 367; Office of the United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, UN Doc A/HRC/27/37 (30 June 2014). See also Bertrand G Ramcharan, 'The Universality of Human Rights' (1994) 53 The Review 105.

[11] Marko Milanovic, *Extraterritorial Application of Human Rights Treaties: Laws, Principles, and Policy* (OUP 2011) 108. See eg International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171, preamble.

[12] US-UK Agreement (n 1) arts 2(1), 3, 5(1)–(2), 6(2)–(3), 8(1)–(2), 9(2), and 10(1)–(2), (5)–(6), and (10).

[13] Jennifer Daskal, 'The Un-Territoriality of Data' (2015) 125 Yale L J 326.

Chapter 1 provides further context, outlining the impetus and operation of the CLOUD Act regime, the methodology of this thesis, and existing literature. Chapter 2 then compares digital privacy rights protections under MLA and the CLOUD Act regime for each of three classes of people: US, UK, and TCNs. Chapter 3 concludes with recommendations for how the Fourth Amendment and Article 8 can be extended extraterritorially to protect TCNs in the context of the CLOUD Act regime.

1.2 The Impetus for and Operation of the CLOUD Act regime

1.2.1 Criminal investigations in the digital era

Human rights, including digital privacy rights, are intimately engaged by criminal investigations.[14] Rights are often seen in tension with interests of security, truth, and justice.[15] In the domestic context, states adopt various *ex ante* and *ex post* mechanisms to balance human rights with societal interests.[16] *Ex ante*—in advance—methods include safeguards aimed at preventing breaches and minimising their impact when they occur, such as through independent court approval of search warrants.[17] *Ex post*—after the fact—mechanisms comprise sanctions against law enforcement officials for misconduct and remedies for victims.[18] In particular, where evidence has been obtained in breach of rights, the most effective remedy will typically be *ex post*, through exclusion of that evidence during criminal proceedings.[19]

---

[14] Stefan Trechsel, *Human Rights in Criminal Proceedings* (OUP 2006) 6–8; Dimitrios Giannoulopoulos *Improperly Obtained Evidence in Anglo-American and Continental Law* (Hart Publishing 2019) 208–211.

[15] Trechsel (n 14) 6–8; Giannoulopoulos (n 14) 28–44; Jenia Iontcheva Turner, 'Regulating Interrogations and Excluding Confessions in the United States: Balancing Individual Rights and the Search for the Truth' in Sabine Gless and Thomas Richter (eds), *Do Exclusionary Rules Ensure a Fair Trial?: A Comparative Perspective on Evidentiary Rules* (Springer 2019).

[16] Giannoulopoulos (n 15) 66 and 251–252.

[17] ibid; Turner (n 15) 97; Sabine Gless and Laura Macula, 'Exclusionary Rules – Is it Time for Change? In Sabine Gless and Thomas Richter (eds), *Do Exclusionary Rules Ensure a Fair Trial?: A Comparative Perspective on Evidentiary Rules* (Springer 2019) 358–359 and 363–366.

[18] Giannoulopoulos (n 15) 251–252; Gless and Macula (n 17) 359–360 and 367–375.

[19] See Giannoulopoulos (n 15) 200–254.

States have however struggled to effectively apply human rights in cross-border contexts.[20] This is increasingly significant as we now live in 'the digital era';[21] electronic data proliferates and flows freely across international borders.[22] Digital evidence is now ubiquitous in criminal investigations.[23] Partly as a result, US and UK law recognise that significant privacy interests apply to searches and seizures of electronic data by law enforcement.[24] These trends are also reflected internationally.[25]

The proliferation of electronic data presents both opportunities and challenges for law enforcement.[26] It is now common for electronic data to be held on our behalf by third party service providers, such as Google, Facebook, and Amazon.[27] US and UK law enforcement often seek target data indirectly through these providers,[28] who are typically

[20] Gane and Mackarel (n 9) 105–108; Currie, 'Human Rights' (n 9) 143 and 171–178; Currie, 'The protection of human rights' (n 9) 29–30 and 38–39; Altwicker (n 9) 584–587.

[21] *The Right to Privacy in the Digital Age* (n 10) [1]–[2].

[22] Daskal, 'Un-territoriality' (n 13) 366–368. See also Andrew Keane Woods, 'Against Data Exceptionalism' (2016) 68 Stan L Rev 729, 754–763.

[23] US Department of Justice [**DOJ**], *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (Version 3, 2009) ix; Home Office, *Crime (Overseas Production Orders) Bill 2018: Overarching Fact Sheet* (September 2018) 3. See also David Anderson, *A Question of Trust: Report of the Investigatory Powers Review* (June 2015) [9.18]; Robert J Currie, 'Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the *Microsoft Ireland* Case the Next Frontier' (2016) 54 Can YB Intl L 63, 74; Els de Busser, 'EU-US Digital Data Exchange to Combat Financial Crime: Fast is the New Slow' (2018) 19 German LJ 1251, 1252; Jennifer Daskal, 'Privacy and Security Across Borders' (1 April 2019) 128 Yale L J Forum 1029, 1032.

[24] *Riley v California* 573 US 373, 393–401 (2014); *Szabó and Vissy v Hungary* (2016) 63 EHRR 3 [53]. See also nn 102–106.

[25] Currie, 'Cross-Border' (n 23) 74–75; Lisl Brunner, 'Digital Communications and the Evolving Right to Privacy' in Molly K Land and Jay D Aronson (eds), *Digital Communications and the Evolving Right to Privacy* (CUP 2018).

[26] Currie, 'Cross-Border' (n 23) 66. See also Jennifer Daskal, 'Law Enforcement Access to Data Across Borders: the Evolving Security and Rights Issues' (2016) 8 J of Nat Sec L & Poly 473, 500.

[27] Anderson (n 23) [6.95]; Daskal, 'Privacy and Security' (n 23) 1033.

[28] Andrew Keane Woods, 'Mutual Legal Assistance in the Digital Age' in David Gray and Stephen E Henderson (eds), *The Cambridge Handbook of Surveillance Law* (CUP 2017) 660–661; Jennifer Daskal, 'Notice and Standing in the Fourth Amendment: Searches of Personal Data' (2017) 26 Wm & Mary Bill Rts J 437, 439. See also DOJ (n 23) 56; Home Office (n 23) 3.

headquartered in the US,[29] but may store data on servers around the world.[30] However, law enforcement have limited methods for obtaining electronic data stored beyond their borders, absent consent or access to a physical device containing that data.[31] Overseas service providers will often refuse direct requests on the basis that providing it would breach applicable 'blocking statutes',[32] such as the US Stored Communications Act (**SCA**) or the UK Investigatory Powers Act 2016 (**IPA**).[33] For example, the SCA generally prohibits disclosure of communications content—ie the full text of an email—although not non-content data, other than to US law enforcement, and in practice service providers may be even stricter, refusing all foreign requests.[34]

When direct requests by a foreign state are made unilaterally and under threat of compulsion, they are also commonly perceived to breach the prohibition against unilateral extraterritorial enforcement jurisdiction at customary international law.[35] A state acts 'extraterritorially' when they act outside their territory.[36] International law distinguishes between *prescriptive* jurisdiction—the ability to make laws about particular matters—and

[29] See Woods (n 28) 661–662 and 663 n9.

[30] Paul W Schwartz, 'Legal Access to the Global Cloud' (2019) 118 Col L Rev 1671, 1686 and 1689–1699.

[31] See DOJ (n 23) 56–59; Home Office (n 23) 3. See generally Law Commission, *Search Warrants* (Com CP No 235, 2018) ch 10.

[32] Anderson (n 23) [11.8]–[11.12], [11.18], and [11.24]; Woods (n 28) 662–663; Jennifer Daskal, 'Borders and Bits' (2018) 71 Vanderbilt L Rev 179, 195–198. See also Kate Westmoreland, 'Are Some Companies "Yes Men" When Foreign Governments Ask for User Data?' (*The Center for Internet and Society*, 30 May 2014) <http://cyberlaw.stanford.edu/blog/2014/05/are-some-companies-yes-men-when-foreign-governments-ask-user-data> accessed 31 July 2020.

[33] Stored Wire and Electronic Communications and Transactional Records Access (Stored Communications Act [**SCA]**), 18 USC §§ 2702(a) and 2703(c); Investigatory Powers Act 2016 [**IPA 2016**], ss 3 and 11. See also HL Deb 20 November 2018, vol 794, col 139.

[34] Westmoreland (n 32); Anderson (n 23) [9.74] and [11.18]; Daskal, 'Borders and Bits' (n 32) 200 n75. See also eg Dropbox, 'Transparency at Dropbox – Reports' (2019) <www.dropbox.com/transparency/reports> accessed 31 July 2020.

[35] Boister (n 5) 328–329; Currie, 'Cross-Border' (n 23) 93–94; Daskal, 'Un-Territoriality' (n 13) 390–391. See generally Michael Akehurst, 'Jurisdiction in International Law' (1972-1973) British Yearbook of Int L 145, 146–148; *Case of the SS Lotus (France v Turkey)* (1927) PCIJ Rep Series A No 10 18–19; *Corfu Channel Case (UK v Albania)* (Merits) [1949] ICJ Rep 4, 34–35; Boister 281–283; Currie, 'Cross-Border' (n 9) 69–74.

[36] Currie, 'Cross-Border' (n 23) 69.

enforcement jurisdiction—the ability to actually enforce or apply these laws.[37] While the international community takes a 'generally permissive approach' to extraterritorial prescriptive jurisdiction, enforcement jurisdiction is traditionally 'strictly territorially bounded'.[38] It is beyond the scope of this thesis to determine the current status of this prohibition. It is however notable that, while some state conduct—including US and UK acts discussed below—may indicate a failure to comply with this prohibition in the digital age,[39] Professor Robert Currie, having extensively surveyed state practice, considers that it remains in force.[40]

1.2.2 Mutual legal assistance (MLA), human rights, and 'the MLAT problem'

Often the only method available to law enforcement to obtain overseas data is MLA.[41] MLA is the international process used by law enforcement to seek and provide assistance internationally.[42] It operates through multilateral conventions, bilateral MLA treaties (**MLATs**) and, absent those, based on understandings of comity.[43] The US and UK have a close MLA relationship, operating both informally, through 'police-to-police cooperation',[44] and formally through an MLAT in force since 1996 (**US-UK MLAT**).[45]

---

[37] ibid 70. See also Law Commission (n 31) [10.139]–[10.143].

[38] Currie, 'Cross-Border' (n 23) 70.

[39] ibid 80–93; Boister (n 5) 328–33; Daskal, 'Borders and Bits' (n 32) 186–198.

[40] Currie, 'Cross-Border' (n 23) 94. See also Stephen Allen, 'Enforcing Criminal Jurisdiction in the Clouds and International Law's Enduring Commitment to Territoriality' in Stephen Allen and others (eds), *The Oxford Handbook of Jurisdiction in International Law* (OUP 2019) 384–386 and 406–410.

[41] DOJ (n 23) 56–57; Home Office (n 23) 24. See also Woods (n 28) 659; Daskal, 'Un-Territoriality' (n 23) 1033–1035.

[42] John AE Vervaele, 'Mutual legal assistance in criminal matters to control (transnational) criminality)' in Neil Boister and Robert Currie (eds), *Routledge Handbook of Transnational Criminal Law* (Routledge 2014) 121–136; Boister (n 5) 313–332.

[43] Vervaele (n 42) 122.

[44] See Boister (n 5) 308.

[45] Treaty between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on mutual legal assistance in criminal matters (signed 4 January 1994, entered into force 6 December 1996) 1967 UNTS 101 (as updated pursuant to various European Union

Requests to the US or UK for electronic data held by service providers require formal MLA, as compulsory legal processes are normally required to obtain such data.[46] As a requesting state is not itself acting extraterritorially, MLA respects the prohibition against unilateral extraterritorial enforcement jurisdiction.[47] MLA has been described as providing a 'built-in-system of double control' and a 'double check' for human rights, because targets theoretically benefit from the rights and constitutional protections of two legal systems.[48]

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 human rights, it more commonly functions as a 'double-edged sword' in which states provide broad assistance for law enforcement internationally but in a context in which human rights protections are reduced if not ignored altogether.[49] As Currie explains, the internationalisation of criminal law through MLA historically developed in 'splendid isolation' from human rights, which largely remain territorially bounded in the eyes of states.[50] In 1989 the European Court of Human Rights (**ECtHR**) recognised that states subject to the ECHR must not extradite in breach of ECHR rights in *Soering v United Kingdom*.[51] However, this principle has not

measures) [**US-UK MLAT**]. See also *R (Terra Services Ltd) v National Crime Agency* [2019] EWHC 3165 (Admin) [16]–[17].

[46] See Boister (n 5) 311.

[47] ibid; Allan (n 40) 385. See also Daskal, 'Un-Territoriality' (n 13) 394; de Busser, 'EU-US' (n 23) 1255–1256.

[48] Lawrence Siry, 'Cloudy days ahead: Cross-border evidence collection and its impact on the rights of EU citizens' (2019) 10 NJECL 227, 232 and 250. See also Christine Galvagna, 'The Necessity of Human Rights Legal Protections in Mutual Legal Assistance Reform' (2019) 9 Notre Dame J of Intl & Comp L 57, 65–66.

[49] See Currie, 'The protection of human rights' (n 9) 30.

[50] ibid 35. See also Currie, 'Human Rights' (n 9) 153; Robert J Currie, '*Charter* Without Borders? The Supreme Court of Canada, Transnational Crime and Constitutional Rights and Freedoms' (2004) 27 Dal LJ 235, 284; Els de Busser, 'The Digital Unfitness of Mutual Legal Assistance' (2017) 28 Sec and Human Rts 161, 168; Altwicker (n 9) 584 and 594.

[51] *Soering v UK* (1989) 11 EHRR 439.

yet been clearly established in relation to MLA,[52] despite extradition technically being a form of MLA itself.[53]

In practice, MLA therefore leads to 'protection gaps'.[54] As set out in Chapter 2, MLA as practised by the US and UK involves fewer *ex ante* and, most significantly, *ex post* protections for rights than equivalent methods used to obtain data domestically. Perhaps most strikingly, states rely on what is known as the 'rule of non-inquiry' to refuse to address credible allegations that human rights have been breached by the other state in an MLA process.[55] This is compounded by the inherent difficulties targets face in gathering evidence of breaches internationally.[56] 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 compared with domestic proceedings.[57] Overall, while there are some signs of recent improvement by US and UK courts, as discussed in Chapter 2, the limited scope of human rights protections for targets during MLA remains a significant concern.

Separately, the 'slow and cumbersome' nature of MLA has also been 'haunting [MLA] procedures for decades'.[58] The UK estimates MLA requests to the US take a year

---

[52] See Ferioli (n 9) 208; *El Gizouli v Secretary of State for the Home Department* [2020] UKSC 10, [2020] 2 WLR 857 [68] (Lord Kerr dissenting but not on this point).

[53] Clive Nicholls and others, *Nicholls, Montgomery, and Knowles on The Law of Extradition and Mutual Assistance* (3rd edn, OUP 2013) [17.01]. Compare Currie, '*Charter* Without Borders? (n 9) 273 n188.

[54] Altwicker (n 50) 584. See also Currie, 'Human Rights' (n 9) 173–4 and 176; Currie, 'Charter Without Borders? (n 9) 280.

[55] Altwicker (n 50) 584. See Currie, 'Human Rights' (n 9) 173-4 and 176; van Hoek and Luchtman (n 9) 2 and 13; Ferioli (n 9) 205–207. See also Woods (n 28) 666.

[56] See van Hoek and Luchtman (n 9) 20.

[57] Ferioli (n 9) 308. See also Sabine Gless, 'Transnational Cooperation in Criminal Matters and the Guarantee of a Fair Trial: Approaches to a General Principle' (2013) 9 Utrecht L Rev 90, 102–103; Robert J Currie, 'Charter Without Borders? (n 9) 278.

[58] Peter Swire and Justin D Hemmings, 'Mutual Legal Assistance In an Era of Globalized Communications: The Analogy To the Visa Waiver Program (2017) 71 NYU Ann Surv of American L 687, 696; de Busser, 'EU-US' (n 23) 1259.

or more.[59] The difficulty of using MLA to obtain electronic data is so widespread it is known generically as 'the MLAT problem'.[60] The delay is attributed to various causes, including perceived insufficient resources invested by the US into MLA.[61] A further problem arises from the evolving ways in which electronic data is stored, which can make it difficult if not impossible to know where to direct requests.[62] The significance of the MLAT problem is heightened by the ever-growing importance of electronic data for criminal investigations outlined above.[63]

1.2.3 Attempts to solve the MLAT problem

In recent years, the MLAT problem—rather than the failings of the process to protect human rights—has led to various calls for reform.[64] While it is beyond the scope of this thesis to canvas all in any detail, two linked US and UK reforms, including the CLOUD Act regime, should be briefly addressed.

From the middle of the last decade, the US and UK have been negotiating the CLOUD Act regime.[65] Concerns with the MLAT problem are long-standing.[66] However,

---

[59] FCO, *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].

[60] Gain Kent, 'The Mutual Legal Assistance Problem Explained' (*Center for Internet and* Society, 23 February 2015) <http://cyberlaw.stanford.edu/blog/2015/02/mutual-legal-assistance-problem-explained> accessed 31 July 2020; Currie, 'Cross-Border' (n 23) 83. See also Anderson (n 23) [11.25]–[12.26]; Boister (n 5) 328–9; Swire and Hemmings, 'Visa Waiver' (n 58) 704–715.

[61] Richard A Clarke and others, *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies* (12 December 2013) 226–227; Bruce Zagaris, 'U.S. Government's Ability to Obtain and Provide International Enforcement Constrained By Budget, Failure to Meet International Standards, and Join International Initiatives' (2015) 31 Intl Enforcement L Reporter 514; Woods (n 28) 664–665; Siry (n 48) 233.

[62] Schwartz (n 30) 1694–1699. See also Currie, 'Cross-Border' (n 23) 82–83.

[63] Text to n 23. See also Woods (n 28) 664–666.

[64] Daskal, 'Law Enforcement Access' (n 26) 476–478; Swire and Hemmings, 'Visa Waiver' (n 58) 715–724; Woods (n 28) 663–673.

[65] Nicola Newsom, 'Crime (Overseas Production Orders) Bill' (*House of Lords Library Briefing*, 5 July 2018) 5.

[66] de Busser, 'EU-US' (n 23) 1259. See also Clarke and others (n 61) 226–229. But see also Woods, 'Mutual Legal Assistance' (n 28) 660.

the CLOUD Act regime's 'direct access' model, by which states seek data directly from overseas service providers, appears to have been first proposed only in 2015 by Sir Nigel Sheinwald, the UK's special envoy on intelligence and law enforcement data sharing, following discussions with overseas service providers and US law enforcement.[67] Along with MLA 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.'[68] This proposal was supported and expanded over the next several years by US academics, most notably Professors Peter Swire, Jennifer Daskal and Andrew Keane Woods.[69] Similar, albeit much less extensive, direct access models are under discussion in the European Union (**EU**) and between members of the Budapest Convention on Cybercrime,[70] and have analogies with earlier national security US-EU data sharing mechanisms.[71]

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.[72] 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*

---

[67] Cabinet Office, *Summary of the Work of the Prime Minister's Special Enjoy on Intelligence and Law Enforcement Data Sharing – Sir Nigel Sheinwald* (25 June 2015). See also Anderson (n 23) 328–9.

[68] Cabinet Office (n 67).

[69] Jennifer Daskal and others, 'Panel 5: Extraterritorial Application of U.S. Law to the Cloud' (Symposium on Government Access to Data in the Cloud, NYU School of Law, 29 May 2015) <www.youtube.com/watch?v=0U5WOYNQCaQ> accessed 31 July 2020; Jennifer Daskal and Andrew Keane Woods, 'Cross-Border Data Requests: A Proposed Framework' (*LawFare* 24 November 2015) <www.lawfareblog.com/cross-border-data-requests-proposed-framework> accessed 31 July 2020; Swire and Hemmings, 'Visa Waiver' (n 58) 720 and 725–738.

[70] Daskal, 'Borders and Bits' (n 32) 198–202; de Busser, 'EU-US' (n 23). See generally Convention on Cybercrime (2001) ETS 185.

[71] See Francesca Bignami and Giorgio Resta, 'Transatlantic Privacy Regulation: Conflict and Cooperation' (2015) 78 L Contemporary Problems 231, 241–247.

[72] Daskal, 'Law Enforcement Access' (n 26) 477–478. See also Currie, 'Cross-Border' (n 23) 91–93.

Ireland.[73] In the UK, powers in the IPA and predecessor legislation purport to be expressly extraterritorial.[74] Although these have yet to be tested in court,[75] UK courts have recently interpreted other laws silent as to their territorial scope as applying extraterritorially over persons with a 'sufficient connection' to the UK.[76] An appeal of the leading decision, *KBR*, is expected to be heard by the UK Supreme Court in late 2020.[77]

These two approaches to addressing the MLAT problem have progressed together. In 2016, contrasting with the approach taken by UK courts, the Second Circuit held in *Microsoft Ireland* that compelling disclosure of Irish data would be an unlawful extraterritorial assertion of SCA powers, contrary to the underlying privacy focus of that legislation.[78] The very next day, the US Department of Justice (**DOJ**) submitted a draft of the CLOUD Act to the US Congress.[79] Although it was not initially progressed, calls for a legislative solution were raised by the Supreme Court during oral argument of *Microsoft Ireland* in February 2018, as well as by Microsoft itself.[80] In response, on 23 March 2018

[73] *Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp* 829 F3d 197 (2nd Cir 2016) [***Microsoft Ireland***]. See also 855 F3d 53 (2nd Cir 2017); *US v Microsoft Corp* 138 S Ct 356 (2017); *US v Microsoft Corp* 138 S Ct 1186 (2018). See generally Justin Hemmings, Sreenidhi Srinivasan, and Peter Swire, 'Defining the Scope of "Possession, Custody, or Control" for Privacy Issues and the CLOUD Act' (2020) 10 J of Natl Sec L and Poly 631, 646–652.

[74] See IPA 2016, ss 9, 41–43, 85, 97, and 139; Anderson (n 23) [6.98].

[75] Anderson (n 23) [6.99].

[76] *R (KBR Inc) v Director of the Serious Fraud Office* [2018] EWHC 2368 (Admin), [2019] QB 675 [63]–[78]; *R (Jimenez) v The First Tier Tribunal (Tax Chamber)* [2019] EWCA Civ 51, [2019] 1 WLR 2956 at [31]–[49]. See also Law Commission, *Search Warrants* (Law Com CP No 235, 2018) [10.125]; Alex Davidson, 'Extraterritoriality and statutory interpretation: the increasing reach of investigative powers' [2020] PL 1.

[77] See *KBR* (n 76).

[78] *Microsoft Ireland* (n 73) 216–221. See also *KBR* (n 76) [60]–[64].

[79] Letter from Peter J Kadzik, US Assistant Attorney Gen, to the Hon Joseph R Biden, President, US Senate (July 15, 2016) https://tinyurl.com/y7b7fhaw> accessed 31 July 2020. See also Letter from Samuel R Ramer, Acting Assistant Attorney General, to Hon Paul Ryan, Speaker, US House of Representatives (24 May 2017) <https://perma.cc/MUT6-A8GC> accessed 31 July 2020.

[80] See Hemmings, Srinivasan and Swire (n 73) 650–652.

Congress enacted the CLOUD Act as part of a consolidated appropriations bill, with very little debate.[81]

The CLOUD Act has two major components.[82] The first gives express extraterritorial scope to the SCA.[83] The second creates a mechanism to allow for international agreements comprising 'the CLOUD Act regime'.[84] Companion legislation, the Crime (Overseas Production Orders) Act 2019 (**COPOA**), was enacted by the UK Parliament in February 2019, again with relatively limited debate.[85] Finally, in October 2019, the US and UK signed the first CLOUD Act regime agreement (**US-UK Agreement**), which may now come into force at any point through an exchange of diplomatic notes.[86]

1.2.4 The CLOUD Act regime and digital privacy protections

Chapter 2 provides an extensive analysis of the operation of the CLOUD Act regime. For present purposes, it is sufficient to summarise the following. A 'core obligation' is 'the removal of any legal barriers that would prevent a [service provider]' in one jurisdiction 'complying with a request from' the other.[87] The regime 'is premised on the notion that [CLOUD Act regime countries] will have the authority under their domestic laws to compel

[81] 163 Cong Rec S7939 (daily ed 1 December 2017); 164 Cong Rec S595 (daily ed 5 February 2018); 164 Cong Rec S1923 (daily ed 22 March 2018). See also *US v Microsoft Corp* 138 S Ct 1186, 1187–1188 (2018).

[82] Hemmings, Srinivasan, and Swire (n 73) 652. See generally Halefom H Abraha, 'Regulating law enforcement access to electronic evidence across borders: the United States approach' (2020) Info & Coms Tech L (forthcoming).

[83] CLOUD Act, § 103(a)(1), enacted at 18 USC § 2713.

[84] ibid § 105(a), enacted at 18 USC § 2523.

[85] See HL Deb 11 July 2018, vol 792, col 927; HL Deb 20 November 2018, vol 794, col 142; HC Deb 18 December 2018, vol 651, col 13.

[86] Greaves and Swire (n 1); US-UK Agreement (n 1) art 16.

[87] HL Deb 20 November 2018, vol 794, col 140; DOJ, 'Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act' (White Paper, April 2019) [**DOJ, *White Paper***] 4; FCO, *Explanatory Memorandum* (n 59) [7]–[8].

production of data held abroad'.[88] In contrast to MLA, requests to overseas service providers for electronic data will now be solely dealt with under the law of the requesting state and by its authorities.[89] Nothing in CLOUD Act regime agreements themselves compels providers to respond to requests; instead, this arises from the law of the requesting state.[90]

The CLOUD Act regime claims to protect digital privacy rights through several overarching procedures.[91] The US Attorney-General must certify a proposed country provides sufficient rights protection,[92] although no statutory mechanism enables this to be challenged.[93] Signatories agree to abide by the digital privacy protections of their own laws.[94] The US-UK Agreement also requires the parties to engage in periodic reviews of their compliance and data handling under it.[95]

There are then two main routes through which digital privacy and other rights are said to be protected in practice, evaluated further in Chapter 2. One is through targeting and minimization procedures.[96] The other protection is provided by service providers, who are permitted to object where they believe a request is improper under the regime.[97] The provider's own state may eventually resolve such requests.[98] Other than in this situation, the CLOUD Act regime presumes that a service provider's own state will normally have

[88] DOJ, *White Paper* (n 87) 6.

[89] See US-UK Agreement (n 1) arts 3(2), 5(1), 5(2), 8(1), 10(2) and 10(5).

[90] See DOJ, *White Paper* (n 87) 5; FCO, *Explanatory Memorandum* (n 59) [7].

[91] See Daskal, 'Law Enforcement Access' (n 26) 495–496; Abraha (n 82) 20–28.

[92] 18 USC § 2523.

[93] ibid § 2523(c); William P Barr, Attorney General, 'Explanation of Each Consideration in Determining that the Agreement Satisfies the Requirements of 18 U.S.C. § 2523(b)' (27 November 2019).

[94] US-UK Agreement (n 1) preamble and arts 2(1) 3(3), 8(1), 9, 10(10).

[95] ibid art 12(1).

[96] ibid arts 1(12), 4 and 7. See Abraha (n 82) 21–22.

[97] US-UK Agreement (n 1) arts 5(11)–(12).

[98] ibid.

no involvement in, or even knowledge of, requests.[99] Where TCNs are targeted, a default obligation to notify their own state also applies.[100]

1.3 Assessing the CLOUD Act Regime Against Digital Privacy Rights

1.3.1 Digital privacy rights, cross-border conduct, and extraterritoriality

This thesis provides a comparative doctrinal analysis, from a rights-based perspective, of the impact of the shift from MLA to the CLOUD Act regime on the digital privacy rights of US persons, UK persons, and TCNs. 'Digital privacy rights' refers here to the rights people have under constitutional mechanisms to retain control over their information when communicating online and in relation to their other electronic content and devices.[101] It is beyond the scope of this thesis to address the global recognition of these rights,[102] or normative arguments in favour.[103] However, such rights clearly apply in the US and UK. The US Supreme Court recognised that the Fourth Amendment—which protects against 'unreasonable searches and seizures'—applied to protect digital privacy rights from improper government conduct in *Riley v California*.[104] 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 to respect for … private and family life, … home and … correspondence'.[105] Outside Scotland, direct UK recognition is less full-throated

---

[99] Andrew Smith, 'Overseas Production Orders: getting up to speed' (2019) 169 NLJ 8730, 9; Abraha (n 81) 21.

[100] US-UK Agreement (n 1) art 5(10).

[101] See *The Right to Privacy in the Digital Age* (n 22).

[102] See eg Ronald J Krotoszynski Jr, *Privacy Revisited: A Global Perspective on the Right to be Left Alone* (OUP 2016); *Dotcom v Attorney-General* [2014] NZSC 199, [2015] 1 NZLR 745; *R v Marakah* 2017 SCC 59, [2017] 2 SCR 608; *Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services* [2019] ZAGPPHC 384, 2020 (1) SA 90 (GP) (appeal pending).

[103] See eg S Warren and L Brandeis, 'The Right to Privacy' (1890) 4 Harv L Rev 193; *The Right to Privacy in the Digital Age* (n 22); Anderson (n 23) [2.8]–[2.13]; Brunner (n 25).

[104] *Riley* (n 24) 393–401. See also *Kyllo v US* 533 US 27 (2001); *US v Jones* 565 US 400 (2012); *Carpenter v US* 585 US __, 138 SCt 2206 (2018).

[105] *C v Chief Constable of the Police Service of Scotland* [2019] CSOH 48, [2019] SLT 875 [101]–[151].

than in the US.[106] However, there is ample ECtHR jurisprudence applying Article 8 in the digital sphere,[107] which must ordinarily be followed by UK courts.[108]

The analysis in this thesis requires engaging with evolving jurisprudence regarding the extraterritoriality of rights, including when the Fourth Amendment and Article 8 apply to states' overseas conduct and, both overseas and generally, the extent to which TCNs and other non-nationals are entitled to their protections.[109] These issues are complex and the extraterritoriality of particular rights may ultimately differ depending on context.[110] This thesis addresses the extraterritoriality of digital privacy rights in the circumstances of cross-border law enforcement. Chapter 2 analyses the operation of these rights under both MLA and the CLOUD Act regime under existing jurisprudence for each of three classes of persons. It shows that existing judicial interpretations limit the application of these rights based on nationality and geography, severely limiting TCNs' enjoyment of digital privacy rights. Reflecting on this, Chapter 3 considers how these limitations can be addressed through reconceptualising each of the Fourth Amendment and Article 8 in the context of the CLOUD Act regime in a manner appropriate for today's digital world.

This regime also interacts with other developing legal issues. A CLOUD Act regime member state may be complicit if another member acts improperly when directly

---

[106] See Orla Lynsky, 'Courts, privacy and data protection in the UK' in Maja Brkan and Evangelia Pscyhogiopodou, *Courts, Privacy and Data Protection in the Digital Environment* (Edward Elgar 2017).

[107] Evangelia Psychogiopoulou, 'The European Court of Human Rights, privacy and data protection in the digital era' in Maja Brkan and Evangelia Pscyhogiopodou, *Courts, Privacy and Data Protection in the Digital Environment* (Edward Elgar 2017). See eg *Zakharov v Russia* (2016) 63 EHRR 17 (GC); *Szabo* (n 24) [53]; *Big Brother Watch v UK* App no 58710/13 (ECtHR, 13 September 2018).

[108] HRA 1998, s 2(1); *R (Ullah) v Special Adjudicator* [2004] UKHL 26, [2004] 2 AC 323 [20]. See also *R (Hallam) v Secretary of State for Justice* [2019] UKSC 2, [2020] AC 279.

[109] See generally Cole (n 10); Milanovic (n 11); Daskal, 'Un-Territoriality' (n 13).

[110] Jacco Bomhoff, 'The Reach of Rights: "The Foreign" and "The Private" in Conflict-of-Laws, State-Action, and Fundamental-Rights Cases With Foreign Elements' (2008) 71 L & Cont Probs 39, 44–49. See eg Peter Swire, Jesse Woo and Deven R Desai, 'The Important, Justifiable, and Constrained Role of Nationality in Foreign Intelligence Surveillance' (Aegis Series Paper No 1901, Hoover Institution, 2019).

enforcing its own orders against the first member's service providers.[111] Similar liability may arise for service providers,[112] as well as, potentially, TCNs' own states in the event these are consulted during the CLOUD Act regime request process.[113] Although worthy of further consideration, these issues are beyond the scope of this thesis, which concentrates on the matters addressed above.

1.3.2 Data protection and other rights

This thesis focuses on the digital privacy rights provided by Article 8 and the Fourth Amendment rather than equivalent data protection rights or other constitutional protections, such as due process / fair trial rights.[114] Article 8 and the Fourth Amendment have historically been perceived to be the key constitutional mechanisms protecting privacy during law enforcement searches in these jurisdictions.[115] While the two are far from identical,[116] they share broad similarities,[117] enabling a rich comparative approach. This focus may also inform Council of Europe countries subject to the ECHR but not the EU, such as Switzerland, as well as other countries with protections similar to the US in this area, such as New Zealand.[118]

---

[111] Patricia L Bellia, 'Chasing Bits Across Borders' (2001) U Chi Legal F 35, 98–99 (citing *Skinner v Railway Labor Executives Assn* 489 US 602, 614–15 (1989)); *El-Masri v Macedonia* (2013) 57 EHRR 25 (GC) [206].

[112] See Allison M Holmes, 'Private actor or public authority? How the status of communications service providers affects human rights' (2017) 22 Comms L 21; *R v Cox* (2004) 21 CRNZ 1 (NZCA) [37]–[38].

[113] Text to n 100.

[114] See US Constitution, Fifth and Fourteenth Amendments; ECHR, art 6. See eg Schwartz (n 30) 1748.

[115] See DOJ (n 23) ix; College of Policing, 'Search powers, and obtaining and executing search warrants' (*Authorised Professional Practice*, last updated 28 April 2020) <www.app.college.police.uk/app-content/investigations/investigative-strategies/search-powers-and-obtaining-and-executing-search-warrants/#action-following-execution> accessed 31 July 2020.

[116] Stefan Sottiaux, *Terrorism and the Limitation of Rights: The ECHR and the US Constitution* (Hart Publishing 2008) 273–312; Bignami and Resta (n 73). See also Peter Swire and DeBrae Kennedy-Mayo, 'How Both the EU and the U.S. Are "Stricter" Than Each Other for the Privacy of Government Requests for Information' (2017) 66 Emory L J 617.

[117] Sottiaux (n 116) 265.

[118] See *Dotcom* (n 102); *R v Alsford* [2017] NZSC 42, [2017] 1 NZLR 710.

The UK is also currently subject to EU data protection rights under the General Data Protection Regulation (**GDPR**), as well as related rights provided for by Articles 7 and 8 of the EU Charter of Fundamental Rights.[119] However, the long-term application of these rights is uncertain following Brexit,[120] and similar rights receive limited protection under US federal law.[121] These rights nevertheless offer extremely fertile ground for future analysis, particularly for EU member states. The Court of Justice of the European Union (**CJEU**), which oversees EU data protection rights, has led much recent development in this area.[122] The GDPR may be an overarching blocking statute in relation to the CLOUD Act regime,[123] and the CJEU's very recent decision *Schrems II*, discussing trans-Atlantic private company data flows, may apply by analogy.[124] In a decision with potentially broad impact, the UK Supreme Court also recently ruled that a UK decision to provide MLA to the US was invalid due to a failure to expressly consider data protection law.[125]

[119] Charter of Fundamental Rights of the European Union [2012] OJ C326/02; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

[120] Karen McCullagh, 'Post-Brexit Data Protection in the UK' in Gloria Gonzalez Fuster and others (eds), *Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics* (Edward Elgar, forthcoming).

[121] Sottiaux (n 116) 265; Paul M Schwartz, 'Global Data Privacy: The EU Way' (2019) 94 NY L Rev 771, 811.

[122] Siofra O'Leary, 'Balancing rights in the digital age' (2018) Irish Jurist 59, 81. See eg *Tele2 SSverige AB v Post-och telestyrelsen (C-203/15)* [2017] QB 771 (CJEU); Case C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd* (CJEU, 16 July 2020) [***Schrems II***].

[123] See eg Jennifer Daskal, '*Microsoft Ireland*, CLOUD Act, and International Law-Making 2.0' (2018) 71 Stan L Rev Online 9, 12–13.

[124] See *Schrems II* (n 122); Henry Farrell and Abraham L Newman, 'Schrems II Offers an Opportunity – If the U.S. Wants to Take It' (*LawFare*, 28 July 2020) <www.lawfareblog.com/schrems-ii-offers-opportunity-if-us-wants-take-it> accessed 31 July 2020.

[125] *El Gizouli* (n 52).

1.3.3 Intelligence sharing, encryption, and hacking

As initial discussions of the CLOUD Act regime included misinformation about its scope,[126] it is important to outline what it does *not* cover. It does not compel decryption by service providers.[127] Nor is it intended to provide a broad mechanism for intelligence collection beyond criminal investigations.[128] The regime is also not a tool for governments to directly 'hack' into electronic devices or servers overseas; data must be obtained through requests to overseas providers.[129]

These issues—encryption, intelligence sharing, and hacking—all engage developing legal issues.[130] They are however beyond the scope of this thesis. At its heart, the CLOUD Act regime is intended to facilitate nations, such as the UK, in accessing electronic data, particularly communications content, from overseas service providers, for criminal investigations and prosecutions. The impact of this regime on digital privacy rights, and reflections on this, is the focus of this thesis.

1.4 Is the CLOUD Act Regime 'Business As Usual' or 'A Race to the Bottom'?

1.4.1 Overall reception

The attitude taken to the CLOUD Act regime largely divides on predictable lines.[131] International interest in joining has been expressed by other 'Five Eyes' countries and close

[126] See eg Steven Swindon, 'Police can access suspects' Facebook and WhatsApp messages in deal with US' (*The Times*, 28 September 2019) <www.thetimes.co.uk/edition/news/police-can-access-suspects-facebook-and-whatsapp-messages-in-deal-with-us> accessed 31 July 2020.

[127] DOJ, *White Paper* (n 87) 18; FCO, *Explanatory Memorandum* (n 59) [17].

[128] 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 Francesca Bignami (ed) *EU Law in Populist Times: Crises and Prospects* (CUP 2020) 335.

[129] See generally Jennifer Daskal, 'Transnational Government Hacking' (2020) 10 J of Natl Sec Law and Poly 677.

[130] nn 127–129.

[131] See Mulligan (n 4) 21–22.

US partners.[132] Australia is already negotiating with the US and has released a draft bill accordingly.[133] Standing in some contrast is the EU. The Commission is currently assessing whether the US-UK Agreement complies with EU law,[134] while EU privacy authorities have expressed concerns.[135] US-EU negotiations to resolve international law enforcement data sharing are ongoing.[136] Global service providers, who have long sought a solution to the conflict of laws problem they face,[137] are broadly supportive,[138] while human rights NGOs appear uniformly critical.[139]

The most extensive consideration has been academic, led by the US. The main commentators there—Swire, Daskal, and Woods—were also the initial advocates of a direct access model, and are thus unsurprisingly strongly supportive.[140] However, it would

---

[132] See Theodore Christakis, 'E-EVIDENCE: THE WAY FORWARD (Summary of the Workshop Held in Brussels on 25 September 2019) (*European Law Blog*, 6 November 2019) <https://europeanlawblog.eu/2019/11/06/e-evidence-the-way-forward-summary-of-the-workshop-held-in-brussels-on-25-september-2019/> accessed 31 July 2020.

[133] DOJ, 'Joint Statement Announcing United States and Australian Negotiation of a CLOUD Act Agreement by U.S. Attorney General William Barr and Minister for Home Affairs Peter Dutton' (7 October 2019) <www.justice.gov/opa/pr/joint-statement-announcing-united-states-and-australian-negotiation-cloud-act-agreement-us> accessed 31 July 2020; Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (Australia).

[134] European Commission, 'Answer to Parliamentary questions given by Mr Reynders' (E-003136/2019, 10 January 2020).

[135] See eg Letter from Andrea Jelinek, Chair of the European Data Protection Board to Members of the European Parliament (15 June 2020) <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out_2020-0054-uk-usagreement.pdf> accessed 31 July 2020.

[136] DOJ, 'Joint US-EU Statement on Electronic Evidence Sharing Negotiations' (26 September 2019) <www.justice.gov/opa/pr/joint-us-eu-statement-electronic-evidence-sharing-negotiations> accessed 31 July 2020.

[137] Anderson [11.22]–[11.24]; Woods (n 28) 673–674.

[138] Letter from Apple and others to Senator Orrin Hatch and others (6 February 2018). See also Brad Smith, Microsoft President 'A call for principle-based international agreements to govern law enforcement access to data' (*Microsoft On the Issues*, 11 September 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/> accessed 31 July 2020.

[139] Letter to Richard W Downing, from Human Rights Watch and others (28 November 2018) <www.hrw.org/news/2018/11/26/letter-us-justice-department-concluding-white-house-should-not-let-uk-demand#> accessed 31 July 2020.

[140] See Jennifer Daskal and Andrew Keane Woods, 'Congress Should Embrace the DOJ's Cross-Border Data Fix' (LawFare, 1 August 2016) <www.lawfareblog.com/congress-should-embrace-dojs-cross-border-data-fix-0> accessed 27 June 2020; Andrew Keane Woods and Peter Swire, 'The CLOUD Act: A Welcome Legislative Fix for Cross-Border Data Problems' (*LawFare*, 6 February 2018)

not be accurate to describe them as uncritical backers. Daskal's position, describing the CLOUD Act regime as 'not perfect' but 'nevertheless a step forward', is representative.[141]

The limited non-US analysis to date emanates from Europe.[142] Discussion has primarily arisen in connection with the EU direct access proposals, given their perceived similarities with the CLOUD Act regime.[143] In stark contrast with the US view, European reaction to date is largely negative, based on rights concerns, as addressed below.[144]

1.4.2 Perceived impact on digital privacy rights

US commentary, building on existing literature on extraterritorial law enforcement data gathering, focuses on the extent to which CLOUD Act regime requests comply with the Fourth Amendment.[145] Most discussion begins (and, largely, ends) with the US Supreme Court judgment *Verdugo-Urquidez*,[146] cited as authority for the proposition that TCNs (including, in this context, UK nationals) do not normally have Fourth Amendment

<www.lawfareblog.com/cloud-act-welcome-legislative-fix-cross-border-data-problems> accessed 31 June 2020.

[141] Daskal, 'Borders and Bits' (n 32) 229. See also Jennifer Daskal, '*Microsoft Ireland* and content regulation: data territoriality and the best way forward' in Horatia Muir Watt and others (eds), *Global Private International Law: Adjudication Without Frontiers* (Edward Elgar 2019) 408–410.

[142] See generally de Busser 'Digital Unfitness' (n 50); de Busser, 'EU-US' (n 23); Siry (n 48); Marco Stefan and Gloria González Fuster, 'Cross-border Access to Electronic Data through Judicial Cooperation in Criminal Matters' (CEPS Paper No 2018-07, November 2018, updated May 2019); Galavagna (n 48). But see also Theodore Christakis, '21 Thoughts and Questions about the UK-US CLOUD Act Agreement (and an Explanation of how it Works – with Charts)' (*European Law Blog*, 17 October 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/> accessed 31 July 2020.

[143] Stefan and Fuster (n 142); de Busser, 'Digital Unfitness' (n 50); 172–178; Siry (n 48) 337–345; de Busser, 'EU-US' (n 23) 1260–1266; Galvagna (n 48) 66–75.

[144] ibid.

[145] Daskal, 'Un-Territoriality' (n 13); Schwartz (n 30) 1708–1714; Swire and Hemmings, 'Overcoming' (n 7) 6–14. See also See Orin S Kerr, The Fourth Amendment and the Global Internet (2015) 67 Stan L Rev 285.

[146] *US v Verdugo-Urquidez* 494 US 259 (1990).

rights.[147] This is, however, an evolving issue, as explored in Chapter 3.[148] Daskal in particular argues for a rejection of the orthodox territorial approach, although her proposed replacement would not fundamentally depart from *Verdugo-Urquidez*.[149]

US commentary on the CLOUD Act regime nonetheless generally at least assumes,[150] if not avowedly defends,[151] the orthodox view. Discussion then turns to the question of incidental collection of US persons' data by the UK through CLOUD Act regime requests to US service providers.[152] There is broad acceptance that such collection is likely if not 'almost certain',[153] and an equally common view that UK law offer less extensive protections than US law, at least in some areas, such as when compared with the 'probable cause' requirement of the Fourth Amendment.[154] Nonetheless, the considered view of Swire, along with Justin Hemmings, is that the scale of incidental collection will be limited, and that the regime overall will therefore likely withstand Fourth Amendment scrutiny.[155] The US government and leading academics further argue that the CLOUD Act regime will raise privacy standards globally, as states will have a 'significant motivation … to increase protections for privacy and civil liberties' to meet the US's

[147] Swire and Hemmings, 'Visa Waiver' (n 50) 737; Jennifer Daskal and Stephen I Vladeck, '"Incidental" Foreign Intelligence Surveillance and the Fourth Amendment' in David Gray and Stephen E Henderson (eds), *The Cambridge Handbook of Surveillance Law* (CUP 2017) 105; Schwartz (n 30) 1709–1710; Swire and Hemmings, 'Overcoming' (n 7) 8. See also eg Secil Bilgic, 'Something Old, Something New, and Something Moot: The Privacy Crisis Under the CLOUD Act' (2018) 32 Harv J of L & Tech 321, 349.

[148] Bomhoff (n 110) 45–46; Daskal, 'Un-Territoriality' (n 13) 378–387; Daskal and Vladeck (n 147) 113–114. See also Kerr (n 145) 302–311.

[149] See Daskal, 'Un-Territoriality' (n 13) 378–387.

[150] ibid 386–387; Schwartz (n 30) 1709–1710; Swire and Hemmings, 'Overcoming' (n 7) 8. See also Kerr (n 145) 301; Daskal and Vladeck (n 147) 105. Compare Bilgic (n 147).

[151] Swire, Woo, and Desai (n 110).

[152] Schwartz (n 30) 1751; Swire and Hemmings, 'Overcoming' (n 7) 10–14.

[153] Daskal, 'Privacy and Security' (n 23) 1048. See also Swire and Hemmings, 'Overcoming' (n 7) 10.

[154] Swire and Kennedy-Mayo (n 116); Daskal, 'Borders and Bits' (n 32) 204. See also eg Eddie B Kim, 'U.S.-U.K. Executive Agreement: Case Study of Incidental Collection of Data Under the CLOUD Act (2020) 15 Wash J of L, Tech & Arts 247, 277–281.

[155] Swire and Hemmings, 'Overcoming' (n 7) 10–14. See also Daskal, 'Un-Territoriality' (n 13), 344–5 and 352. But see also Kim (n 154).

minimum requirements for joining.[156] Daskal suggests that privacy-enhancing amendments to UK surveillance law were made partly for that very reason.[157]

Limited attention is given to *non*-US persons' digital privacy rights beyond the above. This may because, from the US perspective, the primary benefit to them of the CLOUD Act regime is in reducing strain on their MLA system.[158] US officials have expressed doubt as to whether they will ever rely on the CLOUD Act regime, rather than the extraterritorial SCA powers, to make requests,[159] a view critiqued in Chapter 2. Daskal however argues that US courts deciding whether to authorise US requests for overseas data should refuse 'if the disclosure order will violate fundamental rights protections provided by foreign law', drawing on an original proposition of the EU proposals.[160]

A starkly different view is taken across the Atlantic. European academics express significant concerns that rights will be undermined by the shift from MLA.[161] For example, Professor Els de Busser considers that 'the effect of circumventing the safeguards built into the MLA cooperative mechanism is alarming'.[162] She explains that, in contrast with MLA, the country where data is located, which previously would have executed an MLA request for this data under its own law, if appropriate, now 'has no voice in the matter'.[163] The appropriateness of making service providers a responsible for 'safeguarding the interests of the states and individuals involved' also comes in for significant criticism.[164] In

---

[156] DOJ, White Paper (n 87) 13. See also Daskal and Woods (n 140); Jennifer Daskal and Peter Swire, 'Privacy and Civil Liberties Under the CLOUD Act: A Response' (*LawFare*, 21 March 2018) <www.lawfareblog.com/privacy-and-civil-liberties-under-cloud-act-response> accessed 31 July 2020.

[157] Daskal, 'Borders and Bits' (n 32) 204–205.

[158] DOJ, *White Paper* (n 87) 10–11; FCO, *Explanatory Memorandum* (n 59) 5.

[159] See Christakis, '21' (n 142).

[160] Daskal, 'Privacy and Security' (n 23) 1048.

[161] de Busser, 'Digital Unfitness' (n 50) 178–179; de Busser, 'EU-US' (n 23) 1266–1267; Siry (n 48) 238, 240, and 250; Stefan and Fuster (n 142) 3.

[162] de Busser, 'Digital Unfitness' (n 50) 178.

[163] ibid.

[164] ibid 179; Stefan and Fuster (n 142) 50; de Busser, 'EU-US' (n 23) 1266.

particular, de Busser questions whether providers can adequately take into account the interests of TCNs under these direct access models.[165]

1.5 Conclusion

As this Chapter has outlined, the CLOUD Act regime is a new tool for law enforcement, intended to reduce strain on MLA.[166] There is widespread dissatisfaction with MLA as practised by the US and UK. While these states are properly concerned with the speed of MLA, their apparent failure to properly protect human rights during MLA is of even greater significance.[167] Although the US and UK claim that the CLOUD Act regime will be different, both in terms of speed and human rights protections,[168] the literature offers two sharply contrasting views. The US view is generally supportive, viewing the CLOUD Act regime as 'business as usual'. They perceive it as being largely neutral from the perspective of the Fourth Amendment, as those who benefit from it are sufficiently protected through targeting and minimisation, while the world globally gains from the increase in rights as other countries join.[169] The European approach instead expresses significant concerns with the possibility of incoming US requests on the basis that the 'double check' provided by MLA has been replaced solely with review by service providers.[170] Overall, the European position fears a lessening of rights in practice and thus a 'race to the bottom' as the regime expands.

[165] de Busser, 'EU-US' (n 23) 1266–1267.

[166] See generally DOJ, *White Paper* (n 87); FCO, *Explanatory Memorandum* (n 59).

[167] See authorities at nn 49–63.

[168] DOJ (n 6).

[169] Text to nn 145–158.

[170] Text to nn 161–165.

CHAPTER 2

2.1 Introduction

This Chapter evaluates the impact of the CLOUD Act regime on digital privacy rights from the perspective of the three classes of potentially affected persons: US persons, UK persons, and TCNs (ie third country nationals), each of whom is assumed to be physically based in their own territory. It shows that the contrasting positions expressed in the literature in Chapter 1 are each partly right and partly wrong: while rights are largely improved for US and UK persons, they are significantly diminished for TCNs.

Chapter 2 first compares the digital privacy rights afforded to US persons under MLA with the equivalent position they will be in under the CLOUD Act regime. It then repeats the same analysis for UK persons. Each section addresses both *ex ante* and *ex post* protections at the three key stages at which digital privacy rights may be impacted during cross-border data collection: (1) initial steps taken in a requesting country; (2) evaluation and execution of the request in the requested country, and subsequent transmission of the data; and (3) finally, the use of that data as evidence in criminal proceedings in the requesting state.[1] The focus of each section assumes that US persons' data is most likely to be sought from the US and UK persons' data from the UK. Building on this analysis, the final part of Chapter 2 considers the extent to which TCNs' digital privacy rights are protected under each of MLA and the CLOUD Act regime.

2.2 MLA Fails to Protect US Persons' Digital Privacy Rights

2.2.1 Overview

US-UK MLA offers US persons—and, indeed, all persons—significantly fewer protections for digital privacy rights than apply when these states gather evidence domestically.[2] In

[1] Krit Zeegers, *International Criminal Tribunals and Human Rights Law: Adherence and Tension* (Springer 2016) 127. See also Neil Boister, *An Introduction to Transnational Criminal Law* (2nd edn, OUP 2018) 311.

[2] For the US, see *Search and Seizure: A Treatise on the Fourth Amendment* (updated October 2019); DOJ, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (Version 3,

principle, the US is required to act consistently with the Fourth Amendment in its dealings with US persons at all times,[3] but in practice this provides limited protections. The UK, in contrast, will not extend Article 8 protections to US persons during MLA.[4] Although there are some signs of increased willingness by courts to engage with MLA issues,[5] it operates with limited judicial oversight.[6] In particular, both countries continue to apply versions of the 'rule of non-inquiry' to the detriment of targets whose data is sought through MLA.[7]

Overall, due to the above matters, as well as the general confidentiality of MLA requests,[8] US persons have very limited protections in practice during first two stages of the MLA process.[9] These reduced protections may initially be considered insignificant on the basis that the main method by which the digital privacy rights of US persons are upheld under US law is through the *ex post* ability to challenge and exclude evidence in criminal proceedings.[10] However, this exclusion remedy is almost always unavailable for evidence obtained through MLA, leaving US persons with extremely limited protections for digital privacy rights.[11]

2009). 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) [**PACE *Code B***]; Michael Zander, *Zander on PACE: The Police and Criminal Evidence Act 1984* (8th edn, Sweet & Maxwell, 2018) ch 2.

[3] *Weeks v US* 232 US 383, 391–392 (1914); *Elkins v US* 364 US 206, 208–224 (1960); *Berger v State of NY* 388 US 41, 49–64 (1967). See also *Boumediene v Bush* 553 US 723, 765 (2008).

[4] *Human Rights Watch Inc v Secretary of State for the Foreign and Commonwealth Office* [2016] UKIPTrib15_165-ch [56]–[61]; *R (Akarcay) v Chief Constable of the West Yorkshire Police* [2017] EWHC 159 (Admin) [7]–[8] and [35]–[36].

[5] See eg nn 24 and 152.

[6] See eg text to nn 21 and 46.

[7] See eg Robert J Currie, 'Human Rights and International Legal Assistance: Resolving the Tension' (2000) 11 Crim L Forum 143, 171–177; Robert J Currie, 'The protection of human rights in the suppression of transnational crime' in Neil Boister and Robert J Currie, *Routledge handbook of transnational criminal law* (Routledge, Taylor and Francis Group 2015) 37–40.

[8] Text to n 20 below.

[9] Text to nn 12–71 below.

[10] *US v Grubbs* 547 US 90, 99 (2006). Civil remedies may also be available. See *Bivens v Six Unknown Named Agents of Federal Bureau of Narcotics* 403 US 388 (1971).

[11] Text to nn 59–70 below.

2.2.2 Initial US MLA steps

The US MLA process typically begins with a US law enforcement officer contacting the Office of International Affairs (**OIA**) within the US Department of Justice.[12] OIA acts as the US 'central authority' responsible for drafting, approving, and transmitting MLA requests,[13] including for overseas electronic data.[14] The US may only request stored data; interception—known in the US as 'wiretaps'[15]—cannot be requested from the UK.[16] As noted, OIA should act consistently with the US Constitution, including the Fourth Amendment, at all times.[17] This provides a limited degree of *ex ante* protection to US persons.[18]

It is however very difficult to challenge OIA's initial steps and no challenges appear to have ever been successful.[19] Affected persons are very unlikely to ever know an MLA request is made until after the process is complete. Requests are confidential,[20] and

[12] Thomas G Snow, 'The Investigation and Prosecution of White Collar Crime: International Challenges and the Legal Tools Available to Address Them' (2002) 11 Wm & Marty Bill Rts J 207, 227. See also US Department of Justice [**DOJ**], *Justice Manual* (last updated January 2020) [9–13.514].

[13] DOJ (n 12) [9–13.500)–[9–13 525]. See also Snow (n 19), 227–228; T Markus Funk, 'The Key Tools of the Trade in Transnational Bribery Investigations and Prosecutions: Mutual Legal Assistance Treaties (MLATs) and Letters Rogatory' in T Markus Funk and Andrew S Boutros (eds), *Understanding the Global Fight Against Corruption and Graft* (OUP 2019) 550.

[14] DOJ (n 12) [9–13.514] and [9–13.525].

[15] See Wire and Electronic Communications Interception and Interception of Oral Communications [**Wiretap Act**], 18 USC §§ 2510–2523.

[16] Home Office, *Requests for Mutual Legal Assistance in Criminal Matters: Guidelines for Authorities Outside of the United Kingdom* (12th edn, March 2015) 30; Ian Walden, *Computer Crimes and Digital Investigations* (2nd edn, OUP 2016) [5.60].

[17] n 3.

[18] See Funk (n 13) 550.

[19] See n 82.

[20] Treaty between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on mutual legal assistance in criminal matters (signed 4 January 1994, entered into force 6 December 1996) 1967 UNTS 101 (as updated pursuant to various European Union measures) [**US-UK MLAT**], art 7(1). See eg *Grynberg v US DOJ* 302 F Supp 3d 532, 539–540 (SDNY 2018); *ZXC v Bloomberg* [2020] EWCA Civ 611 [16].

typically issued solely by OIA without court input.[21] Even if an affected person were aware of a request, there are normally no meaningful grounds on which they could object.[22] Arguments arising from the MLA treaty between the US and UK (**US-UK MLAT**) are barred.[23] A decision to issue an MLA request may theoretically be challenged on constitutional grounds,[24] but a wide discretion is afforded here to the US government.[25] It would in any event be very difficult if not impossible to establish than an applicant had 'standing' under the Fourth Amendment at this stage, as discussed below.[26]

2.2.3 UK execution of US MLA requests

US MLA requests will be normally be transmitted to the UK Central Authority (**UKCA**) within the UK Home Office,[27] and dealt with under the UK's main MLA statute, the Crime (International Co-operation) Act 2003 (**CICA**).[28] Again, some *ex ante* protection may be provided by UKCA's role,[29] although its task 'should be simple'.[30] The UKCA will refer

---

[21] Funk (n 13) 548. But see 561. See also eg *US v Wilson* 322 F3d 353 (5th Cir 2003).

[22] Text to nn 23–26.

[23] *US v $734,578.82 in US Currency* 286 F3d 641, 659 (3d Cir 2002); *In re Request from United Kingdom Pursuant to Treaty Between Govt of US & Govt of United Kingdom on Mut. Assistance in Criminal Matters in the Matter of Dolours Price* 685 F3d 1, 11–13 (1st Cir 2012) [***Dolours Price (No 1)***]. See also *United Kingdom v US* 238 F3d 1312, 1317 (11th Cir 2001); C Gane and 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' (1994) 4 Eur J Crime, Crim L & Crim Just 98, 105–108.

[24] See *Restatement of the Law – The Foreign Relations Law of the United States* (draft 4th edn, 2020) § 429, Reporters' Note 6. See also eg *US v McLellan* 949 F3d 442, 472–476 (1st Cir 2020).

[25] See *In re Premises Located at 840 140th Ave NE Bellevue Wash* 634 F3d 557, 572 (9th Cir 2011) (citing *Zschernig v Miller* 389 US 429, 432 (1968)).

[26] See *14 Email Addresses* (n 10) 774–775. See also text to n 86 below.

[27] See Home Office (n 16) 4.

[28] Crime (International Co-operation) Act 2003 [**CICA 2003**], ss 13–14 and 17.

[29] CICA 2003, ss 13–14; *R (Hafner) v Home Secretary* [2006] EWHC 1259 (Admin), [2007] 1 WLR 950 [33]; *JP Morgan Chase Bank Natl Assctn v Director of the Serious Fraud Office* [2012] EWHC 1674 (Admin), [2012] Lloyd's Rep FC 655 [25](ii).

[30] *R (Abacha) v Secretary of State for the Home Dept (No 2)* [2001] EWHC Admin 787 [48]. See also *R (Energy Financing Team Ltd) v Bow Street Magistrates' Court* [2005] EWHC 1626 (Admin), [2006] 1 WLR 1316 [11]; *Hafeez v Southwark Crown Court* [2018] EWHC 954 (Admin) [51]; *R (Terra Services Ltd) v National Crime Agency* [2020] EWHC 1640 (Admin) [67]–[69].

a compliant request to law enforcement, who will apply for a court order for the requested data,[31] typically a production order under the Police and Criminal Evidence Act 1984 (**PACE**).[32] Applications must evidence 'reasonable grounds' of applicable matters, such as that the data will be of substantial value to the particular investigation, although courts will conduct a 'more circumscribed' assessment when data is sought through MLA.[33]

Service providers will receive notice of proposed production orders and may therefore conceivably oppose these,[34] albeit on limited grounds.[35] 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.[36] Once the order is obtained and executed, UKCA should provide the requested data to OIA promptly,[37] so long as certain assurances have been given, such as that the data will not be used to facilitate a prosecution resulting in the death penalty.[38] At

[31] CICA 2003, ss 13(1), 14, 15(2) and 17; *Gross v Southwark Crown Court* (Queen's Bench, 24 July 1998); *Terra Services* (n 30) [56]–[66].

[32] Police and Criminal Evidence Act 1984 [**PACE 1984**], ss 9 and sch 1; Home Office, *Crime (Overseas Production Orders) Bill 2018: Overarching Fact Sheet* (September 2018) 2; *R (Secretary of State for the Home Dept) v Crown Court at Southwark* [2013] EWHC 4366 (Admin), [2014] 1 WLR 2529 [26]–[28]; *R (Van Der Pijl) v Secretary of State for the Home Dept* [2014] EWHC 281 (Admin), [2014] Lloyd's Rep 362 [65] and [98]; Michael Zander, *Zander on PACE: The Police and Criminal Evidence Act 1984* (8th edn, Sweet & Maxwell, 2018) [2.23]–[2.41]. See eg *R (NTL Group Ltd) v Ipswich Crown Court* [2002] EWHC 1585 (Admin), [2003] QB 13; *Energy Financing* (n 30) [24](2); *R (River East Supplies Ltd) v Crown Court at Nottingham* [2017] EWHC 1942 (Admin), [2017] 4 WLR 135.

[33] PACE 1984, sch 1; *Van der Pijl* (n 32) [82]. See also *Energy Financing* (n 30) [11]–[17].

[34] PACE 1984, sch 1; *R (British Sky Broadcasting Ltd) v Central Criminal Court* [2014] UKSC 17, [2014] AC 885 [30].

[35] See Zander (n 32) [2–26]–[2–28].

[36] ibid [2–36]–[2–37].

[37] CICA 2003, s 24; *R v Central Criminal Court ex p Propend Finance Property ltd* [1996] 2 Cr App R 26 (QB) 44; *R v Southwark Crown Court ex p Sorsky Defries* (Queen's Bench, 6 July 1995); *Gross* (n 31); *Abacha (No 2)* (n 30) [17]; *JP Morgan* (n 29) [52] and [72]ii). See also *R v Secretary of State for the Home Dept ex p Fininvest SpA* [1997] 1 WLR 743 (QB) 758; *R (Abacha) v Secretary of State for the Home Dept (No 1)* [2001] EWHC Admin 424 [1]; *R (Evans) v Director of the Serious Fraud Office* [2002] EWHC 2304 (Admin), [2003] 1 WLR 299 (QB) [24].

[38] *El Gizouli v Secretary of State for the Home Dept* [2020] UKSC 10, [2020] 2 WLR 857 [26] (Lord Kerr dissenting but not on this point).

each of these UK stages, there is a residual discretion to decline to progress a request, although this is rarely exercised.[39]

The main method available to persons seeking to object to claimed rights breaches in the UK at this point is through judicial review. This is separate from opposing a PACE application directly, although a decision to grant an application may be at the heart of such a judicial review.[40] Judicial review of each of the above UK MLA stages has been sought,[41] with occasional success.[42] US targets would have standing to seek judicial review,[43] although practically review would have little point after transmission of data to OIA. Additionally, judicial review of such investigatory steps is entertained only rarely,[44] and then typically on strict *Wednesbury* grounds, under which a decision will be set aside only if it was 'so unreasonable that no reasonable authority could ever have come to it'.[45] UK courts will exercise even further restraint in 'the context of mutual assistance'.[46] They 'take on trust' that a requesting state has acted lawfully and reasonably in making the request, absent 'compelling' proof otherwise.[47] A claim that the US had breached a target's Fourth Amendment rights would be met with a UK court responding that this is 'a matter

---

[39] For discretion at authorisation, see *Propend* (n 37) 33; *Abacha (No 2)* (n 30) [17]; *JP Morgan* (n 29) [53]; *R (BSG Resources Ltd) v Director of Serious Fraud Office* [2015] EWHC 1813 (Admin) [3]. For discretion before transmission, see *Fininvest* (n 37) 758]; *Zardari v Secretary of State for the Home Dept (No 2)* (Queen's Bench, 9 April 2001); *Abacha (No 1)* [1]; *Evans* (n 37) [24]. See also *River East* (n 32) [106].

[40] See eg *Terra Services* (n 30).

[41] See eg *Fininvest* (n 37) 748, 755, and 758; *Gross* (n 31); *Abacha (No 1)* (n 39); *Omega Group Holding Ltd v Kozeny* EWCA Civ 798, [2005] 1 WLR 104 [51]; *R (Van der Pijl) v Crown Court at Kingston* [2012] EWHC 3745 (Admin), [2013] 1 WLR 2706 [1].

[42] *Defries* (n 37); *R v Secretary of State for the Home Dept ex p KM* (Divisional Court, 7 April 1998); *Gross* (n 31); *Van der Pijl* (n 41). See also *Superior Import / Export Ltd v Commissioners for HMRC* [2017] EWHC 3172 (Admin) [85].

[43] See eg *Propend* (n 37) 29.

[44] See *Energy Financing* (n 32) [24](9).

[45] *Associated Provincial Picture Houses Ltd v Wednesbury Corp* [1948] 1 KB 223 (EWCA). See *Fininvest* (n 37) 747; *JP Morgan* (n 29) [55]; *Fawwaz v Secretary of State for the Home Dept* [2015] EWHC 166 (Admin) [69].

[46] *Van Der Pijl* (n 41) [81]–[82].

[47] *JP Morgan* (n 29) [53], [66], and [72]; *Malabu Oil and Gas Ltd v Director of Public Prosecutions* (Crown Court, 15 December 2015) [44]. See also *Abacha (No 2)* (n 30) [27] and [44].

for the requesting state'.[48] 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'.[49]

There appears to be no ability for US persons to directly object to MLA in UK courts on the basis that their digital privacy rights were breached.[50] They will normally be barred from raising Article 8 or other ECHR claims.[51] Although there is no direct authority from the ECtHR, [52] in 2015, the UK Investigatory Powers Tribunal ruled in *Human Rights Watch Inc v Secretary of State for the Foreign and Commonwealth Office* that the UK owes no obligations under Article 8 to persons physically outside UK territory.[53] In 2017, the High Court of England and Wales similarly rejected an Article 8 objection to a UK decision to provide MLA to Northern Cyprus on the basis that the claimant—then in Northern Cyprus—was not 'within the jurisdiction of the UK for the purposes of the ECHR'.[54] It is unlikely that equivalent protections would apply under common law.[55] Aside from the recent Scottish judgment referred to in Chapter 1,[56] UK courts have been reluctant to extend

[48] *JP Morgan* (n 29) [53]; *R v Secretary of State for the Home Dept ex p Zardari* (Queen's Bench, 11 March 1998). See also *Calder v Frame* [2006] HCJAC 62, [2007] JC 4 [31] and [34]; *Fawwaz* (n 45) [61].

[49] *Abacha (No 2)* (n 30) [50] (citing *Zardari* (n 48) (Lord Bingham CJ)). See also *Omega (No 2)* (n 41) [45].

[50] Text to nn 51–57.

[51] *Human Rights Watch* (n 4) [56]–[61]; *Akarcay* (n 4)] [35]–[36]. See also *R (Zagorski) v Secretary of State for Business, Innovation and Skills* [2010] EWHC 3110, [2011] HRLR 6 [57]; *R (Sandiford) v Secretary of State for Foreign and Commonwealth Affairs* [2013] EWCA Civ 581, [2013] 1 WLR 2938 [33]–[38]; *El Gizouli* (n 38) [69] (Lord Kerr dissenting but not on this point).

[52] Francesca Bignami and Giorgio Resta, 'Human Rights Extraterritoriality: The Right to Privacy and National Security Intelligence' in Eyal Benvenisti and Georg Nolte (eds), *Community Interests Across International Law* (OUP 2018) 376.

[53] *Human Rights Watch* (n 4) [58].

[54] *Akarcay* (n 4) [35]–[36].

[55] See Kirsty Hughes, 'A Common Law Constitutional Right to Privacy – Waiting for Godot?' in Mark Elliott and Kirsty Hughes (eds) *Common Law Constitutional Rights* (Hart Publishing 2020).

[56] *C v Chief Constable of the Police Service of Scotland* [2019] CSOH 48, [2019] SLT 875 [101] to [151].

privacy rights in this manner.[57] Alternatively, although beyond the scope of this thesis, data protection claims may also be available.[58]

2.2.4 Subsequent US use of data

Once UKCA transmits the requested data back to the US, OIA will review and then forward it to the requesting US law enforcement officer.[59] Under the 'rule of speciality', it can then be deployed only for the proceedings for which it was sought in accordance with US law.[60] Normally, a defendant seeking to protect digital privacy rights could at this stage rely on the 'principal judicial remedy' the Fourth Amendment provides,[61] the exclusionary rule.[62] However, this will rarely be available in this context as set out below.

The Fourth Amendment typically requires US law enforcement to act reasonably and obtain a warrant—which must be sufficiently particular and backed by probable cause[63]—before conducting a search and seizure infringing on reasonable expectations of privacy.[64] US courts increasingly recognise reasonable expectations of privacy over much electronic data, including the contents of emails held by service providers.[65] Although subject to exceptions,[66] the exclusionary rule makes evidence obtained in breach of these

---

[57] See Brice Dickson *Human Rights and the United Kingdom Supreme Court* (OUP 2013) 228.

[58] See *El Gizouli* (n 38).

[59] Snow (n 13) 228.

[60] *US v Rommy* 506 F3d 108, 129 (2d Cir 2007) See also US-UK MLAT, above n 20, art 7(2).

[61] *US v Strieff* 579 US __, __, 136 SCt 2056, 2061 (2016). See also *Mapp v Ohio* 367 US 643, 651–652 (1961); *Herring v US* 555 US 135 (2009) (Ginsburg J dissenting).

[62] *Weeks* (n 3) 398; *Mapp* (n 61) 650–660; *US v Leon* 468 US 897, 909–910 (1984). But see *Herring* (n 61) 139–147.

[63] *Kentucky v King* 563 US 452, 479 (2011). See also *Illinois v Gates* 462 US 213, 230–241 (1983).

[64] *Kyllo v US* 533 US 27, 31–35 (2001). See also *Grady v North Carolina* 575 US 306, 310 (2015).

[65] *US v Warshak* 631 F3d 266, 288 (6th Cir 2010); US House of Representatives [**HOR**] *Email Privacy Act* (HOR 114th Congress, 2d Sess, 114–528) 9; *Carpenter v US* 583 US __, __, 138 S Ct 2206, 2219–2222 (2018). See generally *Riley v California* 573 US 373, 393–401 (2014).

[66] *Leon* (n 62). See also *Herring* (n 61) 139–147.

obligations generally inadmissible.[67] It is 'designed to safeguard Fourth Amendment rights generally through its deterrence effect'.[68] It applies to evidence obtained directly from an illegal search and seizure as well as 'fruits of the poisonous tree', meaning later-discovered evidence 'derivative of an illegality'.[69]

The Fourth Amendment will almost always be inapplicable in the MLA context, however.[70] This is because 'the exclusionary rule, as a deterrent sanction, is not applicable where … a foreign government commits the offending act.'[71] Both direct and derivative MLA evidence are instead normally admissible under the 'international silver platter' doctrine.[72] 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 illegality.[73] The international silver platter doctrine has also been applied where data was seized overseas but not reviewed until transmitted to US territory.[74] The only exceptions to this doctrine are where the foreign law enforcement's acts 'shocks the conscience', an extremely high bar,[75] or where US law enforcement were so substantially involved that the acquisition became a 'joint venture' with foreign officials.[76]

---

[67] *Mapp* (n 61) 655.

[68] *Herring* (61) 139–140.

[69] *Wong Sun v US* 371 US 471, 484–485 (1963); *Segura v US* 468 US 796, 804 (1984).

[70] See eg *US v Adler* 605 F Supp 2d 829, 837–838 (WD Tex 2009); *US v Omar* Crim No 09–242 (MJD/FLN), 2012 WL 2277821 (D Minn, 18 June 2012) *2–3; *US v Evtimov* No 14 CR 131–4, 2016 WL 1181828, *3–5 (ND Ill, 28 March 2016) *3–5.

[71] *US v Janis* 428 US 433, 455 n31 (1976) (citing *US v Stonehill* 274 F Supp 420 (SD Cal 1966)). See also *US v Odoni* 782 F3d 1226, 1237–40 (11th Cir 2015).

[72] *US v Lee* 723 F3d 134 (2d Cir 2013); *US v Emmanuel* 565 F3d 1324, 1330 (11th Cir 2009); *US v Stokes* 726 F3d 880 (7th Cir 2013); Jay V Prabhu, Alexander P Berrang, and Ryan Dickey, 'When Your Cyber Case Goes Abroad: Solutions to Common Problems in Foreign Investigations' (2019) 67 DOJ J Fed L and Prac 167, 177–179. See also *US v Defreitas* 701 F Supp 2d 297, 304 (EDNY 2010).

[73] See *US v Vilar* Case No S3 05–CR–621 (KMK), 2007 WL 1075041 *59 (SDNY 4 April 2007).

[74] See eg *Defreitas* (n 72) 306 n11.

[75] *US v Getto* 729 F3d 221, 228–230 (2d Cir 2013).

[76] See Prabhu, Berrang and Dickey (n 72) 177–178. Compare *Lee* (n 72) 140. See also Orin S Kerr, 'The Fourth Amendment and the Global Internet' (2015) 67 Stan L Rev 285, 297–301.

In the rare scenarios that the Fourth Amendment is applied in this context, most US courts have held that only the Fourth Amendment's reasonableness requirement will apply abroad; warrants are not required.[77]

2.2.5 Reciprocal UK requests for US persons' data

The reciprocal position, where US persons' data is sought by the UK through MLA, can be outlined briefly, as UK MLA requests are detailed further below.[78] Overall, although *ex ante* statutory protections constrain UK officials' acts in principle, the UK's own acts when seeking data through MLA—ie first making a request and subsequently receiving and deploying data in criminal proceedings—provide limited protections in practice for digital privacy rights. US persons are relatively worse off than their UK counterparts, as existing UK authority, outlined above, holds that the UK owes no obligation to protect US persons' digital privacy rights under Article 8.[79]

US persons also have limited protections even at the second MLA stage, when UK MLA requests are executed in the US. Some *ex ante* protection is obtained from screening of incoming MLA requests by OIA and law enforcement for compliance with US law, including the Fourth Amendment.[80] US MLA actions may theoretically be challenged on constitutional grounds, even where statutory requirements have been met.[81] However, as noted, no challenges have been successful.[82]

---

[77] *In re Terrorist Bombings of US Embassies in E Africa* 552 F3d 157, 167–173 (2d Cir 2008); *Stokes* (n 72) 891–893; Prabhu, Berrange and Dickey (n 72) 140–141. See also Kerr (n 74) 301.

[78] nn 154–196 below.

[79] *Human Rights Watch* (n 4) [56]–[61]; *Akarcay* (n 4)] [35]–[36].

[80] Peter Swire and Justin D Hemmings, 'Mutual Legal Assistance In an Era of Globalized Communications: The Analogy To the Visa Waiver Program' (2017) 71 NYU Ann Surv of American L 687, 735–736.

[81] Compare *City of Ontario v Quon* 560 US 746, 764 (2010) with *Carpenter v US* 585 US __, __, 138 S Ct 2206, 2221–2222 (2018). See also eg *US v Scully* 108 F Supp 3d 59, 88 (EDNY 2015).

[82] *In re Premises* (n 25) 574; *Dolours Price (No 1)* (n 23) 15; *In re Request from the United Kingdom to the Treaty Between the Government of the US and the Government of the United Kingdom on Mut Assistance in Criminal Matters in the Matter of Dolours Price* 718 F3d 13, 23 (1st Cir 2013) [***Dolours Price (No 2)***]; *McLellan* (n 24) 471–472. See also *Palmat International Inc v Holder* No 12-20229-CIV, 2013 WL 594695 (SD Florida, 13 February 2013); *In re Ex parte Petition of the Republic of Turkey for an Order Directing*

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 Stored Communications Act (**SCA**) and enabling statutes.[83] They will often be issued with delayed or no notice to a target,[84] leaving only the service provider able to object. Yet the provider can do so on limited grounds only; they apparently cannot vicariously assert a target's Fourth Amendment rights.[85] Even when targets attempt to bring challenges, US courts to consider the issue have held that targets lack 'Fourth Amendment standing' to challenge such SCA warrants prior to execution,[86] leaving targets with no way to uphold their digital privacy rights at this stage.

2.3 The CLOUD Act Regime Enhances US Persons' Digital Privacy Rights

2.3.1 Overview

US persons' digital privacy rights will be significantly enhanced through the CLOUD Act regime. Most significantly, the 'international silver platter' doctrine should no longer apply.[87] US persons will thus regain the principal judicial remedy of the Fourth Amendment, the exclusionary rule.[88] Additionally, all stages of the law enforcement data-

Discovery from Hamit Çiçeek Pursuant to 28 USC § 1782 No 2:19-CIV-20107-ES-SCM, 2020 WL 2539232 (DNJ 18 May 2020) *6.

[83] SCA, 18 USC §§ 2701–2713; Foreign Evidence Efficiency Act, 18 USC § 3512; and Assistance to foreign and international tribunals and to litigants before such tribunals, 28 USC § 1782. See Funk (n 11) 554–557; *Restatement (4th)* (n 23) § 429, Comment (b). See also eg *In re United States for an Order Pursuant to 18 USC § 2703(D)* Misc Action No 17–2682 (BAH), 2018 WL 1521772 *1 n1 (DDC 8 March 2018).

[84] 18 USC §§ 2703(b), (c)(3) and 2705; *In re US* 665 F Supp 2d 1210, 1224 (D Or 2009).

[85] 18 USC §§ 2703(d); *Microsoft Corp v United States Dept of Justice* 233 F Supp 3d 887, 915–16 (WD Wash 2017). See also Aviv S Halpen, 'Secret Searches: The SCA's Standing Conundrum' (2019) 17 Mich L Rev 1696, 1700; Jennifer Daskal, 'Notice and Standing in the Fourth Amendment: Searches of Personal Data' (2018) 46 Wm & Mary Bill Rts J 437. See generally *Rakas v Illinois* 439 US 128, 133–134 (1978); *US v Padilla* 508 US 77, 81 (1993).

[86] *In re Search of Records, Info, & Data Associated with 14 Email Addresses Controlled by Google LLC* 438 F Supp 3d 771, 774–775 (ED Mich 2020); *US v Information Associated With Email Account (Warrant)* Crim Act No 19MJ2012, 2020 WL 1499264 *3–5 (ED PA 27 March 2020).

[87] Compare text to nn 71–76.

[88] See *Strieff* (n 61) 2061.

gathering process must now comply with constitutional mechanisms protecting digital privacy rights, whereas the UK denied such benefits to US persons when executing requests.[89]

The degree to which US persons' digital privacy rights will be improved in practice turns in part on the method the US adopts to implement the CLOUD Act regime. These rights may also be implicated by incoming UK CLOUD Act regime requests. Nonetheless, the overall impact of the regime for US persons represents a tangible improvement compared with the MLA status quo.

2.3.3 The CLOUD Act regime appear to be rights-enhancing for US persons

Despite claims to the contrary,[90] there are two scenarios in which the US is likely to use its new CLOUD Act regime powers. First, as addressed below, the US-UK Agreement enables the US to expand its enforcement jurisdiction over UK service providers holding data that previously would have been accessible only through MLA.[91] This includes not only stored data, but intercept data, which the US was barred from seeking from the UK through MLA.[92] Secondly, the US may use the regime to obtain data from providers already within its jurisdiction where these providers may otherwise have objected that

[89] Text to nn 51–57.

[90] See Theodore Christakis, '21 Thoughts and Questions about the UK-US CLOUD Act Agreement (and an Explanation of how it Works – with Charts)' (*European Law Blog*, 17 October 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/> accessed 31 July 2020 (apparently referencing Richard Downing, Deputy Assistant Attorney General, DOJ, Remarks during panel discussion titled 'Globalization of Criminal Evidence' (Privacy + Security Academy, Washington DC, 15 October 2019)). See also The Overseas Production Orders and Requests for Interception (Designation of Agreement) Regulations 2020 [**Designation Regulations**], *Explanatory Memorandum* [7.4] and [12.3].

[91] See eg *Omar* *1 (n 70); *US v Killen* 729 Fed Appx 703, 714 n7 (11th Cir 2018); *US v Minava* No CV 17-359 (KM), 2019 WL 1615549 *5 (DNJ 16 April 2019); US' Trial Brief 7–8 *US v Nikulin* 2020 WL 1910377, No CR 16 – 00440 WHA (ND Cal, 3 March 2020). See also Prabhu, Berrang, and Dickey (n 72) 170–171.

[92] Compare Home Office (n 16) 30.

disclosing would breach a UK blocking statute,[93] as the US-UK Agreement requires these statutes to be lifted for CLOUD Act regime requests.[94]

As a matter of both international and US law,[95] the US-UK Agreement enables the US to extend its enforcement jurisdiction over UK service providers by consent given by the UK.[96] US law previously permitted US law enforcement to obtain orders against overseas providers only where they were independently subject to the US's 'personal jurisdiction'.[97] Now, as the US has stated, it 'will have reciprocal access, under a U.S. court order, to data from UK communication service providers'.[98] The fact the US-UK Agreement enables expanded jurisdiction is emphasised by the UK approach, discussed below.[99] Unfortunately, recent US comments have confused this issue. The US has repeatedly claimed that neither the CLOUD Act nor any bilateral agreement 'by itself' would establish jurisdiction over foreign service providers.[100] Such statements are strictly

[93] See eg IPA 2016, ss 3 and 11.

[94] FCO, *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* (CP 178, 3 October 2019) [**US-UK Agreement**] arts 5(1) and 10(1). See also IPA 2016, s 52; Designation Regulations (n 90), s 2(b); Jennifer Daskal, 'The Opening Salvo: The CLOUD Act, e-Evidence Proposals, and EU–US Discussions Regarding Law Enforcement Access to Data across Borders' in Francesca Bignami (ed) *EU Law in Populist Times: Crises and Prospects* (CUP 2020) 326.

[95] Michael Akehurst, 'Jurisdiction in International Law' (1972-1973) British Yearbook of Int L 145, 146–148; *Restatement* (n 24) § 431; *Reid v Covert* 354 US 1, 15 (1957); *Wilson v Girard* 354 US 524 (1957); Patricia L Bellia, 'Chasing Bits Across Borders' (2001) U Chi Legal F 35, 80–86. See also Theodore Christakis and Kenneth Propp, 'The Legal Nature of the UK-US CLOUD Agreement' (Cross-Border Data Forum, 20 April 2020) <www.crossborderdataforum.org/the-legal-nature-of-the-uk-us-cloud-agreement> accessed 31 July 2020.

[96] US-UK Agreement (n 94) arts 3(1) and 10(1).

[97] See Justin Hemmings, Sreenidhi Srinivasan, and Peter Swire, 'Defining the Scope of "Possession, Custody, or Control" for Privacy Issues and the CLOUD Act' (2020) 10 J of Natl Sec L and Poly 631, 654–666.

[98] DOJ, 'U.S. and UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online' (3 October 2019) <www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists>. See also Paul M Schwartz, 'Legal Access to the Global Cloud' (2018) 118 Colum L Rev 1681, 1748.

[99] Text to 209–215 below. See also *Water Splash Inc v Menon* 581 US __, __, 137 S Ct 1504, 1512 (2017).

[100] DOJ, *Promoting Public Safety, Privacy and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act* (White Paper, April 2019) [**DOJ, *White Paper*]** 5; Richard W Downing, 'Prospects for Transatlantic Cooperation on the Transfer of Electronic Evidence to Promote Public Safety' (Academy of European Law Conference, London, UK, 5 April 2019).

true but misleading. While neither mechanism, standing alone, expands US jurisdiction, they *enable* such expansion, primarily by requiring each party to remove blocking mechanisms in their domestic law.[101]

General guidance about making CLOUD Act regime requests can be found in the US-UK Agreement.[102] Each state has a 'Designated Authority'—assumed here to be the OIA—occupying a central role.[103] Outgoing requests will be reviewed by OIA for compliance with US law and the US-UK Agreement.[104] They will then be transmitted directly to the UK service provider holding the data.[105] This is a key change from MLA, replacing review by the UK state and its courts.[106] Concerns with the adequacy of this second step in terms of protecting rights are discussed below in relation to TCNs.[107] Based on equivalent UK estimates, the UK service provider will likely take up to a week to transmit the data back.[108] OIA will review and then transmit the data to the requesting law enforcement agent.[109] At that point, the data can be deployed in criminal proceedings as if obtained domestically.[110] While the extent of Fourth Amendment protections over this process is uncertain, as set out below, the Fourth Amendment will at least now apply

[101] US-UK Agreement (n 94) arts 3(1) and 10(1). See Frederick T Davis and Anna R Gressel, 'Storm Clouds or Silver Linings? The Impact of the U.S. Cloud Act' [Fall 2018] Litigation 47, 49–50; Jennifer Daskal, 'Privacy and Security Across Borders' (1 April 2019) 128 Yale L J Forum 1029, 1042. See also *Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp* 855 F3d 53, 74 (2d Cir 2017) (Cabranes J dissenting).

[102] See also Haleform H Abraha, 'Regulating law enforcement access to electronic evidence across borders: the United States approach' (2020) Info & Comms Tech Law (forthcoming).

[103] US-UK Agreement (n 94) arts 1(8) and 5(5)–(12).

[104] ibid arts 5(5)–(6).

[105] ibid art 5(5) and 10(2).

[106] See Daskal, 'Opening Salvo' (n 94) 358.

[107] See nn 282–305 below.

[108] See Crime Overseas Production Orders Act 2019 (UK) [**COPOA**], s 5(5).

[109] See Snow (n 13) 228.

[110] Compare text to n 60.

generally to all constrain all government conduct in this process,[111] providing greater *ex ante* protections compared with MLA.[112] US persons' digital privacy rights are likely to be particularly enhanced if requests are made under the SCA and Wiretap Act, given the protections these statutes provide.[113]

Most significantly, the final stage of CLOUD Act regime requests—reliance on the data in criminal proceedings—also provides significantly enhanced *ex post* protections for US persons compared with MLA. Previously, MLA data would be generally admissible under the 'international silver platter' doctrine.[114] Under this doctrine, US courts have admitted evidence obtained through methods that would breach the Fourth Amendment if occurring domestically, including searches without a warrant in breach of foreign law.[115] Unless US agents are directly involved in foreign acts, little short of torture by a foreign state appears sufficient to warrant exclusion.[116] However, this doctrine should no longer apply to US requests under the CLOUD Act regime, as US law enforcement will now be in control of the entire process.[117] The Supreme Court clarified as long ago as 1960 that 'silver platter' exceptions have no application in such contexts.[118] Given the important role the exclusionary rule plays in protecting US persons' digital privacy rights,[119] this gain is significant.

---

[111] n 3.

[112] See text to n 4.

[113] nn 140–141.

[114] Text to nn 71–77.

[115] *US v Peterson* 812 F2d 486, 491 (1987). See also *US v Mitro* 880 F2d 1480, 1483 (1989); *Stokes* (n 72) 891; *Getto* (n 75) 228.

[116] *Getto* (n 75) 229. See also eg *US v Fernandez-Caro* 677 F Supp 893, 895 (SD Tex 1987).

[117] *See Reid* (n 95) 9 (citing *Best v US* 184 F2d 131, 138 (1st Cir 1950)); *In re Terrorist Bombings* (n 77) 167; *Stokes* (n 72) 890–891.

[118] *Elkins* (n 3) 208.

[119] n 61.

2.3.2 Implementation uncertainties do not alter this conclusion

How the US intends to exercise its new CLOUD Act regime powers remains unclear. The US-UK Agreement allows requests using 'a legal instrument issued under the domestic law of the Issuing Party' and accompanied by a related certification.[120] Daskal argues that these requests would be extraterritorial under US law and that "there is not – as of now – any explicit legal authority in U.S. law that would enable" them.[121] Even if correct, this does not undermine the focus of this thesis: the US-UK Agreement enables the US to now exercise expanded enforcement jurisdiction over UK providers subject only, Daskal says, to passing explicit legislative authority, which the US could readily do.[122] There are good reasons for the US to exercise such jurisdiction and it is therefore important to consider the effect of this on digital privacy rights.[123]

It is however not clear that the US does require further legislation. First, it is arguable that, at least in respect of stored data, the US can now issue extraterritorial SCA orders. As a result of a CLOUD Act amendment, outlined in Chapter 1, a service provider subject to US jurisdiction must now disclose data under the SCA 'within such provider's possession, custody, or control' from anywhere in the world.[124] This, together with the US-UK Agreement, may extend the SCA's powers over UK providers.[125] Supporting this interpretation, a related CLOUD Act amendment to the SCA included a reference to 'foreign' service providers for the first time.[126]

---

[120] US-UK Agreement (n 94) arts 1(1) and 5(7)–(8). See also arts 5(1) and 10(2).

[121] Daskal, 'Privacy and Security' (n 101) 1042. See also Jennifer Daskal, 'Setting the Record Straight: the CLOUD Act and the Reach of Wiretapping Authority under US law' (*Cross-Border Data* Forum, 1 October 2018) <www.crossborderdataforum.org/setting-the-record-straight-the-cloud-act-and-the-reach-of-wiretapping-authority-under-us-law> accessed 31 July 2020.

[122] Text to nn 95–101. See Daskal, 'Privacy and Security' (n 101) 1042.

[123] Text to nn 90–94.

[124] 18 USC § 2713.

[125] Text to nn 95–101.

[126] CLOUD Act, § 103(b) (implemented as 18 USC § 2703(h)).

Secondly, although US courts have overwhelmingly held (prior to the SCA amendment outlined above) that the SCA and Wiretap Act lack extraterritorial force,[127] 'extraterritoriality' has a distinct US law meaning.[128] Most US courts consider an SCA request to be territorial so long as the provider discloses data within US territory, regardless where it was retrieved from.[129] They have also adopted a 'listening post' theory, by which intercepts will not be extraterritorial so long as the US agent is listening within US territory,[130] even if the intercept is otherwise entirely foreign.[131] If methods were established to enable UK service providers to disclose or route data within US territory in response to SCA or Wiretap Act orders, these orders may therefore be within the scope of these statutes. A failure to comply would be punishable by contempt.[132]

Finally, even if CLOUD Act regime requests were extraterritorial under US law and the provisions of the SCA and Wiretap Act were unavailable, the US may nonetheless already be able to make such requests.[133] US courts are often permissive when reviewing overseas US government acts, holding that the US is 'not constrained' by domestic statutes

[127] See eg *Peterson* (n 115) 492; *In re Search Warrant Issued to Google Inc* 264 F Supp 3d 1268, 1271–72 (ND Al 2017).

[128] See Jennifer Daskal, 'The Un-Territoriality of Data' (2015) 125 Yale L J 326, 354–365. See also eg *US v Hasbajrami* 945 F3d 641, 655 (2d Cir 2019).

[129] *In re Search Warrant Issued to Google Inc* (n 127) 1271–72; *In re Search Warrant to Google Inc* Mag No 16-4116, 2017 WL 2985391, at *3–4 (DNJ, 10 July 2017). Compare *Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp* 829 F3d 197, 219–221 (2nd Cir 2016) [***Microsoft Ireland***].

[130] *US v Rodriguez* 968 F2d 130, 136 (2d Cir 1992); *US v Jackson* 849 F3d 540, 551-2 (3d Cir 2017). See also *Dahda v US* 584 US__, __, 138 SCt 1491, 1495 and 1499 (2018).

[131] *US v Cano-Flores* 796 F3d 83, 86 (DC Cir 2015); *US v Cosme* No 1-cr-394-WQH, 2011 WL 3740337 (SD Cal 2011); *US v Rodriguez-Serna*, No 18CR3739 WQH, 2019 WL 4214389 (SD Cal 5 September 2019). See also Jennifer Daskal, 'Correcting the Record: Wiretaps, the CLOUD Act, and the US-UK Agreement' (*JustSecurity*, 31 October 2019) <www.justsecurity.org/66774/correcting-the-record-wiretaps-the-cloud-act-and-the-us-uk-agreement/> accessed 31 July 2020. But see *US v Caro* No CR 12-964-DMG, 2015 WL 13358324 *2 (CD Cal 2 December 2015).

[132] See eg *Microsoft Ireland* (n 129), 200–201.

[133] Compare Daskal, 'Privacy and Security' (n 101) 1042.

such as the Wiretap Act when acting extraterritorially.[134] Further, similar powers under MLATs are generally considered self-executing without additional legislation.[135] As noted, US courts have held that the US government only needs to comply with the Fourth Amendment's reasonableness requirement when acting overseas.[136] Neither the Fourth Amendment nor the US-UK Agreement appears to require a warrant for US CLOUD Act regime requests.[137] It may therefore be permissible for the US to request US persons' data using 'any number of lesser forms of legal process', falling far short of the SCA and Wiretap Act's protections.[138] While neither statute contains an applicable exclusion remedy,[139] the SCA contains 'Fourth Amendment-like protections' for orders seeking stored data,[140] while the Wiretap Act is even stricter, requiring a 'probable cause-plus' standard.[141] For reasons explored in Chapter 3, the rationale for *not* extending the Fourth Amendment's warrant requirement appears inapplicable here. Under existing case law, however, the use of such lesser forms of legal process appears both possible and concerning for US persons' digital privacy rights. Overall, a shift to the CLOUD Act regime would nonetheless still be rights-enhancing for US persons, given the renewed availability of the exclusionary rule.

---

[134] *US v Verdugo-Urquidez* 494 US 259, 265–275 (1990); *US v Vega* 826 F3d 514, 541 (DC Cir 2016). See also eg *US v Gorshkov* No CR00-550C, 2001 WL 1024026 *3 (WD Wash 23 May 2001); *US v Lugo Morales* No 4:17-CR-203-ALM-KPJ, 2019 WL 1561901 *2 (ED Tex 21 March 2019).

[135] See eg *Rommy* (n 60) 128.

[136] n 77.

[137] US-UK Agreement (n 94) arts 5(2) and 10(2).

[138] See Albert Gidari, 'More Questions About the CLOUD Act and the US-UK Agreement – Can the US Direct UK Providers to Wiretap Their Users in Third Countries?' (*The Center for Internet and Society*, 13 November 2019) <http://cyberlaw.stanford.edu/blog/2019/11/more-questions-about-cloud-act-and-us-uk-agreement-can-us-direct-uk-providers-wiretap> accessed 31 July 2020.

[139] 18 USC § 2707; 18 USC § 2518; *US v Steiger* 318 F3d 1039, 1046 (11th Cr 2003); *US v Clenney* 631 F3d 658, 667 (4th Cir 2011).

[140] Orin S Kerr, 'A User's Guide to the Stored Communications Act, and A Legislator's Guide to Amending It' (2004) 72 Geo Wash L Rev 1208, 1214.

[141] Peter Swire and DeBrae Kennedy-Mayo, 'How Both the EU and the U.S. Are "Stricter" Than Each Other for the Privacy of Government Requests for Information' (2017) 66 Emory L J 617, 644–646.

2.2.3 Reciprocal UK requests raise only limited concerns

Neither of the two ways that US persons' digital privacy rights may be impacted by UK actions under the CLOUD Act regime appear to outweigh the significant gains they obtain for digital privacy rights.

First, the US-UK Agreement prohibits the UK from directly targeting US persons and requires targeting and minimisation procedures to be developed accordingly.[142] Swire and Hemmings consider any incidental collection of US persons' data will therefore be insignificant.[143] The scope for subsequent use is, however, broad. The UK may use any incidentally collected US persons' data where this is directly or indirectly relevant to the UK's own investigations.[144] The UK may also distribute incidentally collected data to the US where it 'relates to significant harm, or the threat thereof, to the United States or to U.S. Persons'.[145] The US could theoretically then deploy that data freely under the 'international silver platter doctrine'.[146]

As discussed in Chapter 1, the UK may also intercept data in the US under UK legal standards that are considered significantly less protective than the requirements of the Wiretap Act.[147] The impact of the UK's increased powers to intercept under the US-UK Agreement is a challenging topic generally, partly addressed below.[148] Its particular impact on US persons is however considered low.[149]

---

[142] US-UK Agreement (n 94) arts 4(3)–(4) and 7.

[143] Swire and Justin Hemmings, 'Overcoming Constitutional Objections to the CLOUD Act' (*American Constitution Society*, Issue Brief, February 2020) 7–9.

[144] US-UK Agreement (n 94) art 7(3).

[145] ibid art 7(5).

[146] Text to nn 73–77.

[147] See eg Swire and Kennedy-Mayo (n 141) 644–646.

[148] Text to nn 239–252.

[149] Swire and Hemmings (n 94) 12–13. See also *Hasbajrami* (n 128) 666–668.

2.4 UK Persons' Digital Privacy Rights Are Similarly Limited Under MLA

2.4.1 Overview

UK persons receive diminished protections for their digital privacy rights during MLA compared with how these rights are protected during domestic evidence collection.[150] In principle, the UK must act consistently with Article 8 when dealing with UK persons (at least within UK territory).[151] There is also increasing recognition that ECHR rights are engaged during MLA.[152] However, UK persons have very limited scope to uphold these rights in practice during all three stages of the MLA process.[153]

Overall, UK persons are in a similar, albeit less severe, position as US persons during MLA. UK courts' application of the rule of non-inquiry, the general confidentiality of MLA, and the limited rights afforded to UK persons in the US, leave UK persons with significantly reduced rights protections.

2.4.2 Initial UK MLA steps

Requests for stored data held by US service providers, including the contents of communications, generally require a formal MLA request under CICA, the UK's main MLA statute.[154] Requests are normally made by UK law enforcement or, occasionally, courts.[155] Law enforcement work with UKCA to prepare and transmit an MLA request to

---

[150] n 2.

[151] HRA 1998, s 6; *Aston Cantlow and Wilmcote with Billesley Parochial Church Council v Wallbank* [2003] UKHL 37, [2004] 1 AC 546 [7]. See also *Human Rights Watch* (n 4) [58].

[152] *Hafner* (n 29) [28].

[153] Text to nn 154–205.

[154] CICA 2003, s 7; Home Office (n 16) 30. See also *R v Redmond* [2006] EWCA Crim 1744, [2009] 1 Cr App R 25 [25]; Crown Prosecution Service [**CPS**], 'International Enquiries' *The Code for Crown Prosecutors* (1 July 2019) <www.cps.gov.uk/legal-guidance/international-enquiries> accessed 31 July 2020; Andrew Keane Woods, 'Mutual Legal Assistance in the Digital Age' in David Gray and Stephen E Henderson (eds), *The Cambridge Handbook of Surveillance Law* (CUP 2017) 663.

[155] CICA 2003, s 7; CICA 2003 (Designation of Prosecuting Authorities) Order 2004, r 2; CPS (n 154).

OIA.[156] UKCA must be satisfied that proposed requests meet certain CICA threshold requirements.[157] All UK public authorities involved in transmitting an MLA request for a UK person's data should comply with Article 8 at all times.[158] These requirements theoretically give some *ex ante* protections for UK persons.

There is however very little ability to meaningfully enforce these obligations in practice. Court approval of MLA requests is not required.[159] Judicial review will 'rarely' be permitted.[160] UK law enforcement are under much less onerous obligations when issuing an MLA request than when applying for a domestic production order or similar compulsory process.[161] UK authorities are not under a 'duty of candour' when preparing MLA requests.[162] Courts also accept that requests may be more broadly drafted than equivalent domestic applications.[163] As requests are confidential, targets are also very unlikely to be aware when a request is proposed.[164] To date, UK courts have merely assumed, but never actually determined, that a decision to transmit an MLA request engages privacy rights protected by Article 8.[165] They have then readily concluded that any interference is justified.[166]

---

[156] CPS (n 154).

[157] CICA 2003, s 7(5). See *R v Foxley* [1995] 2 Cr Ap R 523 (EWCA) 532; *Re McIntrye* [2018] NIQB 79 [33] (appeal pending).

[158] n 151.

[159] CICA 2003, s 7; Alex Mills, 'Crime (Overseas Production Orders) Act 2019: The Increasing Relevance of UK Investigatory Powers to those Advising Businesses and Individuals' (2019) 9 JIBFL 624, 624.

[160] *R (Unaenergy Group Holding) v SFO* [2017] EWHC 600 (Admin), [2017] 1 WLR 3302 [24] and [34](iii).

[161] ibid; Mills (n 161) 624.

[162] *Unanergy* [32]–[38] and [53]; *McIntyre* (n 157) [43]–[45] See also *Foxley* (n 157) 533–534; *HM Advocate v Megrahi (No 2)* [2000 SLT 1399 (HCJ) [2].

[163] *Rea's (Winston Churchill) Application* [2015] NICA 8, [2016] NI 203 [14]–[16]. See *Fininvest* (n 37) 752; *Foxley* (n 157) 533–534. See also eg *Amalgamated Metal Trading Ltd v City of London Police Financial Investigation Unit* [2003] EWHC 703 (Comm), [2003] 1 WLR 2711 [9].

[164] CPS (n 154). See also n 20.

[165] *Winston Churchill* (n 163) [23]–[26]; *McIntyre* (n 157) [51] and [52](xi). See also *Unaenergy* (n 160) [37].

[166] *Winston Churchill* (n 163) [25]; *McIntyre* (n 157) [51].

2.4.3 US execution of UK MLA requests

Once OIA receives UKCA's MLA request (and again before it transmits data back), it will review for compliance with US law.[167] OIA will then refer the request to US law enforcement to apply for an order. As noted, requests for stored data are sought under a combination of the SCA and specific statutes facilitating MLA.[168] US courts have been described as 'gatekeepers' in ensuring that US law is complied with during MLA.[169] While US authorities also have a discretion to refuse assistance, there is a strong presumption requests will be granted.[170] Nonetheless, the roles of OIA, the SCA, and US courts again provide a degree of *ex ante* protection for UK persons. The privacy protections provided by the SCA apply equally to US persons and foreigners.[171]

Ex post protections are however largely non-existent. UK persons are unlikely to be aware when an SCA order is sought or be found to have 'standing' to dispute it in any event.[172] Service providers may object on limited grounds only.[173] While constitutional challenges to decisions to provide MLA are theoretically available,[174] UK persons suffer from the fundamental limitation that, on current US authority, they normally have no Fourth Amendment rights whatsoever,[175] and thus no way to meaningfully protect their

---

[167] Woods (n 154) 663–664; Swire and Hemmings, 'Visa Waiver' (n 80) 698–700 and 735–736.

[168] n 83.

[169] Funk (n 13) 556–557.

[170] ibid 557 (citing *In re Premises* (n 25) 571).

[171] *Suzlon Energy Ltd v Microsoft Corp* 671 F3d 726, 729 (9th Cir 2011). See also Kerr, 'User's Guide' (n 140) 1214; *In re Toft* 453 BR 186, 197–8 (Bankr SDNY 2011).

[172] Text to 86.

[173] nn 84–85.

[174] n 85. But see also text to n 86.

[175] *Verdugo-Urquidez* (n 134) 265–275. See also Ian R Connor, 'Peoples Divided: The Application of United States Constitutional Protections in International Criminal Law Enforcement' (2002) 11 Wm & Mary Bill of Rts J 495, 507–508; *Agency for Intl Devpt v Alliance for Open Society Intl Inc* 591 US __, __, 140 SCt 2082, 2086–2087 (2020).

digital privacy rights. As outlined in Chapter 1, the Supreme Court case *Verdugo-Urquidez* is commonly interpreted by US courts as authority in the context of the Fourth Amendment that non-resident aliens only 'receive constitutional protections when they have come within the territory of the United States and developed substantial connections with this country'.[176] While the meaning of 'substantial connections' remains debated,[177] *Verdugo-Urquidez* is typically applied as preventing US courts from even assessing whether US acts against non-US persons comply with the Fourth Amendment.[178]

2.4.4 Subsequent UK use of data

Once UKCA receives the requested data, it will provide it to the requesting law enforcement officer who can deploy it in the proceedings for which it was sought, subject to standard admissibility rules,[179] as well as the 'rule of speciality'.[180] Unlike the US, an exclusion remedy remains theoretically available for UK persons whose digital privacy rights have been breached during MLA.[181] This may either be sought directly under s 78 of PACE during criminal proceedings or through an application for judicial review.[182] While the ECHR only applies to its member states,[183] the ECtHR has also recognised that reliance by a member state on evidence unlawfully obtained by a foreign state may breach

[176] *Verdugo-Urquidez* (n 134) 271. See eg *US v Zakharov* 468 F3d 1171, 1179 (9th Cir 2006); *Emmanuel* (n 72) 1331–1332; *US v Rojas* 812 F3d 382, 397 (5th Cir 2016). See also Prabhu, Berrang, and Dickey (n 72) 177–178; Laura K Donohue, 'The Fourth Amendment in a Digital World' (2017) 71 NYU Ann Survy Am L 553, 665. But see also Kerr (n 76) 292–294.

[177] Donohue (n 176) 667. See eg *Ibrahim v Dept of Homeland Sec* 669 F3d 983 (9th Cir 2012); *Omar* (n 70) *3–4.

[178] See eg *Emmanuel* (n 72) 1331–1332; *Rojas* (n 176) 398.

[179] See eg *R v Iqbai* [2002] EWCA Crim 2714 [8].

[180] See n 60 above; CICA 2003, s 9(2); US-UK MLAT, art 7(2); *Gohil v Gohil* [2012] EWCA Civ 1550, [2013] 2 WLR 1123 [36]–[42]. See also *XYZ v HM Revenue & Customs* [2012] EWHC 1645 [25].

[181] See CPS (n 154).

[182] See eg *Unaenergy* (n 160).

[183] *Soering v UK* (1989) 11 EHRR 439 [86].

that member's own ECHR obligations.[184] However, compared with the ordinary US approach, a much less generous approach to exclusion is taken in the UK.[185] Other than when procured through torture,[186] evidence obtained in breach of ECHR rights remains generally admissible; it will be excluded only where, taking into account all the circumstances, its admission would breach a defendant's fair trial rights protected by Article 6.[187]

The application of the rule of non-inquiry by UK courts further restricts the ability to exclude MLA evidence. Just as UK courts assume foreign states have acted lawfully and reasonably in requesting MLA,[188] they will equally assume that the UK's own MLA requests have been properly executed by foreign states, including fellow ECHR member states and others.[189] Under UK law, questions about whether evidence was gathered in breach of foreign law must normally be litigated in the state where this occurred;[190] UK courts will entertain such issues rarely and then only on narrow grounds.[191] Other than for breaches of the rule of speciality,[192] the only circumstance in which UK courts have suggested MLA evidence may be inadmissible was where the foreign state that provided the evidence subsequently alleged that its own laws had been breached during MLA.[193]

---

[184] *Echeverri Rodriguez v Netherlands* App no 43286/98 (ECtHR, 27 June 2000). Compare *Chinoy v UK* App no 15199/89 (Commission Decision, 4 September 1991). See also Aukje AH van Hoek and Michiel JJP Luchtman, 'Transnational cooperation in criminal matters and the safeguarding of human rights' (2005) 1(2) Utrecht L Rev 1, 18.

[185] Compare *Mapp* (n 61) 650–660 with *R v P* [2002] 1 AC 146 (HOL) 158–162.

[186] *Othman v United Kingdom* (2012) 55 EHRR 1 [263]–[267].

[187] *Khan v United Kingdom* (2001) 31 EHRR 45 [25]–[28] and [34]–[40]; *R v P* (n 185) 158–162; Zander (n 32) [14-04].

[188] Text to nn 46–49.

[189] For ECHR states, see *Winston Churchill* (n 163) [20]; *Unaenergy* (n 160) [35](ii). For others, see *Foxley* (n 157) 535; *Torres v HM Advocate* 1998 SLT 811 (HCJ) 815–6; *Re Quattrocchi* [2004] EWCA Civ 40 [27]. See also van Hoek and Luchtman (n 184) 3.

[190] *Quattrocchi* (n 189) [27]; *Malabu* (n 47) [63]. See also *Torres* (n 189) 816.

[191] See *Torres* (n 189) 816.

[192] See eg *Gohil* (n 180) [41].

[193] *R v I* [2008] EWCA Crim 3062 [23]–[27].

Overall, although not as prohibitive as the US 'international silver platter' doctrine,[194] and regardless of its merits,[195] the application of the rule of non-inquiry leaves UK persons with significantly reduced digital privacy rights during MLA.[196]

2.4.5 Reciprocal US requests for UK persons' data

Where the US requests UK persons' data through MLA from the UK, the process will be similar as set out above.[197] UK persons have slightly greater scope to object to the execution of an MLA request by the UK as they can allege Article 8 breaches.[198] Article 8 is engaged through the use of the UK's compulsory powers during MLA.[199] The ECtHR has ruled that member states have breached Article 8 in the context of executing MLA requests.[200] However, UK courts have overwhelmingly held that interferences with Article 8 are justified during MLA given the public interest in prosecuting crime and on the basis that CICA provides robust safeguards.[201]

In contrast, at the final stage of MLA, when the evidence is deployed in criminal proceedings, UK persons will be in an even worse position than their US equivalents. While US persons at least theoretically may raise exceptions to the 'international silver platter' doctrine,[202] UK persons cannot. *Verdugo-Urquidez* is interpreted as prohibiting a US court from applying the Fourth Amendment, no matter how egregious a breach of

---

[194] Text to nn 71–72.

[195] Zeegers (n 1) 138. See also van Hoek and Luchtman (n 184) 25.

[196] See Currie, 'Human Rights' (n 7) 173; Zeegers (n 1) 136–138.

[197] Text to nn 12–70.

[198] Compare *Akarcay* (n 4) [35]–[36].

[199] *Hafner* (n 29) [21]–[22]; *Home Dept v Southwark Crown Court* (n 32) [8].

[200] *MN v San Marino* (2016) 62 EHRR 19 [51]–[55] and [74]–[85]; *Visy v Slovakia* App no 70288/13 (ECtHR, 16 October 2018) [37]–[47].

[201] *Calder v Frame* (n 48) [29]–[32]; *Hafner* (n 29) [18]–[26]; *H v Lord Advocate* [2011] HCJAC 77, 2011 SCL 978 [46]; *BSG Resources* (n 39) [18]. See also *Warner v Verfides* [2008] EWHC 2609 (Ch), [2009] Bus LR 500 [19]; *Home Dept v Crown Court at Southwark* (n 32) [8].

[202] Text to nn 71–72.

digital privacy rights.[203] Although UK persons benefit from the SCA's protections,[204] the SCA does not provide an exclusion remedy in this context.[205]

2.5 The Cloud Act Regime Likely Also Enhances UK Persons' Digital Privacy Rights

2.5.1 Overview

The CLOUD Act regime is likely to also significantly enhance the rights of UK persons, at least in respect of stored data requests. This shift is not as pronounced as for US persons, because the status quo UK persons face under MLA is not as rights-limiting. Nonetheless, UK persons will materially benefit and for similar reasons. UK persons will gain from increased *ex ante* protections for digital privacy rights provided by COPOA's detailed statutory scheme. It is also arguable that Article 8 will now apply to all UK actions.[206] Most significantly, UK courts should no longer apply the 'rule of non-inquiry' when seeking data under the CLOUD Act regime, improving *ex post* protections.[207]

While the regime appears to be rights-enhancing from the perspective of stored data—despite greater scope for UK persons' data to be obtained through US requests—a definitive conclusion as to its overall impact on UK persons' digital privacy rights must await further developments. The regime enables the UK to enforce various controversial intercept powers extraterritorially.[208] The extent to which this undermines UK persons' digital privacy rights is a complex, evolving issue that is ultimately beyond the scope of this thesis.

---

[203] See eg *US v Fantin* 130 F Supp 2d 385, 391 (WDNY 2000).

[204] n 171.

[205] 18 USC § 2708; *US v Gasperini* 894 F3d 482, 488-9 (2d Cir 2018).

[206] Compare text to nn 167–168. See also text to nn 188–196.

[207] See text to nn 188–196.

[208] Text to n 239–252.

2.5.2 The CLOUD Act regime largely appears to be rights-enhancing for UK persons

It is undisputed that the UK will use its new expanded enforcement jurisdiction under the CLOUD Act regime to facilitate access to data from US service providers such as Microsoft, Google, Apple, and similar.[209] While alternative powers may be available,[210] the UK enacted specific legislation, COPOA, to enable outgoing CLOUD Act regime requests for precisely these purposes.[211] COPOA allows requests to overseas providers operating in CLOUD Act regime countries,[212] even where they have no UK presence whatsoever.[213] These providers were previously 'beyond the reach of existing domestic court powers' and their data could be compelled only through MLA.[214] COPOA represents a 'broad assertion of authority', albeit one 'premised on consent'.[215]

COPOA, which for these purposes must be interpreted consistently with the US-UK Agreement,[216] allows for orders similar to PACE production orders.[217] US service providers may be compelled to disclose data for a UK criminal investigation where threshold requirements are made out.[218] Applications may be without notice and orders may prohibit disclosure to the target.[219] Many US service providers will otherwise disclose

---

[209] See Nicola Newsom, 'Crime (Overseas Production Orders) Bill' (*House of Lords Library Briefing*, 5 July 2018) 3; HC Deb 30 January 2019 vol 653, cols 852 and 859–860.

[210] Criminal Justice Act 1987, s 2; *R (KBR Inc) v Director of the Serious Fraud Office* [2018] EWHC 2368 (Admin), [2019] QB 675. See also Alex Davidson, 'Extraterritoriality and statutory interpretation: the increasing reach of investigative powers' [2020] PL 1.

[211] See Newsom (n 209).

[212] COPOA 2019, ss 1(2) and (5).

[213] ibid s 4(8)(a).

[214] ibid *Explanatory Notes* [2]–[4].

[215] Jennifer Daskal, 'Transnational Government Hacking' (2020) 10 J Nat Sec L & Poly 677, 695.

[216] *Assange v Swedish Prosecution Authority* [2012] UKSC 22, [2012] 2 AC 471 [10], [98], [112], [115] and [122].

[217] See COPOA 2019, *Explanatory Notes* [7]; Home Office (n 32) 1.

[218] COPOA 2019, ss 1 and 4; Criminal Procedure Rules 2015 [**CPR 2015**] r 47.68; Mills (n 159) 624–625. See also Designation Regulations (n 90); US-UK Agreement (n 94) art 1(7).

[219] COPOA 2019, ss 8 and 12–13; CPR 2015, rr 47.68(1)(e) and 2. See also Mills (n 159) 624.

to targets as a matter of course.[220] Orders must be served by the UK's designated authority, presumably UKCA.[221] The provider will normally have up to one week to provide the data, absent objections.[222] A failure to comply may again be punished as contempt.[223] The data may then be deployed as if obtained domestically.[224]

This model appears to increase *ex ante* protections for UK persons' digital privacy rights. UK court oversight over outgoing MLA requests is typically non-existent and limited at best.[225] US oversight occurs in a context in which the underlying target—a UK person—would typically have no Fourth Amendment rights.[226] Under COPOA, requests must be independently approved by a UK court.[227] Potential overreliance on COPOA's nondisclosure powers is concerning,[228] but would still leave UK persons in an improved position, given the overarching confidentiality of MLA.[229] Additionally, while there are concerns as to the appropriateness of the role of service providers under the CLOUD Act regime, addressed below,[230] UK persons nonetheless appear to be an improved position overall.

---

[220] See eg Brad Smith, 'A call for principle-based international agreements to govern law enforcement access to data' (*Microsoft On the Issues*, 11 September 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/> accessed 31 July 2020; *US v Information Associated With Email Account (Warrant)* (n 86) *1.

[221] COPOA 2019, s 9. See also s 14; Home Office, *Crime (Overseas Production Orders) Bill: Impact Assessment* (HO315, 11 May 2018) 12.

[222] COPOA 2019, s 4(5); *R (Director of the Assets Recovery Agency) v He* [2004] EWHC 3021 (Admin) [8].

[223] CPR 2015, r 47.71.

[224] See eg Andrew Smith, 'Overseas Production Orders: getting up to speed' (2019) 169 NLJ 8730, 10.

[225] Text to nn 159–166.

[226] Text to nn 175–178.

[227] COPOA 2019, s 4.

[228] Compare Rebecca Niblock, 'On its way: The UK-US Bilateral Data Access Agreement' (*Kingsley Napley Criminal Law Blog*, 19 June 2020) <www.kingsleynapley.co.uk/insights/blogs/criminal-law-blog/on-its-way-the-uk-us-bilateral-data-access-agreement> accessed 31 July 2020, with Criminal Procedure (Amendment No 2) Rules 2019, *Explanatory Memorandum* [7.12].

[229] Text to nn 20 and 164.

[230] Text to nn 282–305.

The *ex post* protection provided by the ability to exclude evidence, typically under s 78 of PACE, is also greater. The 'rule of non-inquiry' should no longer apply;[231] instead, UK law enforcement will be expected to fully justify their use of compulsory powers.[232] Furthermore, Article 8 would apply to, at least, the UK's use of data obtained through COPOA as evidence in criminal proceedings against UK persons.[233] Article 8 'demands more than compliance with the relevant provisions of domestic law' and its application may therefore provide additional protections.[234]

Whether Article 8 applies to the UK's acts under COPOA directly is unclear. These are very likely 'extraterritorial' under UK law,[235] yet the ECHR typically only applies to constrain member states when acting within their own territory.[236] One exception is where member states exercise a foreign government's 'public powers' with that government's 'consent, invitation or acquiescence' under a treaty or similar agreement.[237] The US-UK Agreement would appear to be precisely such an agreement, as it enables to the UK to exercise enforcement jurisdiction against US service providers where previously US assistance through MLA would have been required.[238] On that basis, Article 8 would apply to all UK acts under COPOA, further strengthening UK persons' digital privacy rights.

---

[231] Text to nn 188–196.

[232] See PACE *Code B* (n 2) [1.3].

[233] See *Rodriguez* (n 184).

[234] *Calder v Frame* (n 48) [32]. See also *Halford v United Kingdom* (1997) 24 EHRR 523 [49].

[235] *KBR* (n 210) [30]; *R (Jimenez) v First Tier Tribunal (Tax Chamber)* [2019] EWCA Civ 51, [2019] 1 WLR 2956 [48]; Davidson (n 210). See also Home Office, *OFS* (n 32).

[236] ECHR, art 1; *Bankovic v UK* (2007) 44 EHRR SE5 [73]–[74]; See also David Anderson, *A Question of Trust: Report of the Investigatory Powers Review* (June 2015) [5.37]–[5.39].

[237] *Al-Skeini v United Kingdom* [2011] 53 EHRR 18 (GC) (n 236) [135]. See also *Tomanovic v Foreign and Commonwealth Office* [2019] EWHC 3350 (QB), [2020] 4 WLR 5 [93]–[100].

[238] See US-UK Agreement (n 94) arts 5(5) and 10(2).

2.5.3 Increased intercept powers may significantly undermine UK persons' rights

The UK has very broad and controversial intercept powers,[239] most recently codified in the IPA. These extend extraterritorially, expressly requiring overseas service providers to assist with intercepts.[240] The US-UK Agreement offers the UK greater scope to compel overseas assistance,[241] as it permits the UK to enforce certain of these extraterritorial powers against US providers.[242]

Intercept powers are undoubtedly highly intrusive interferences with digital privacy rights.[243] However, the UK asserted these powers prior to the CLOUD Act regime.[244] What is relevant here is not the impact of these powers on digital privacy rights generally but the extent to which such rights are undermined due to the UK's increased ability to exercise these powers extraterritorially through the CLOUD Act regime. From that perspective, there are reasons for concern. Relative to the equivalent US Wiretap Act powers,[245] the IPA's provisions are extensive and opaque,[246] in part because the UK generally bans the use of intercept evidence in criminal proceedings.[247] The UK specifically negotiated for interception abilities within the US-UK Agreement and is likely to now rely on these clauses extensively given the proportion of UK data US providers

[239] See eg Paul F Scott, *The National Security Constitution* (Hart Publishing 2018) 59–104. See also Anderson (n 236) [13.31]–[13.35].

[240] IPA 2016, ss 42, 43(3), 85, 97, and 139.

[241] Compare Anderson (n 236) [6.95]–[6.99].

[242] IPA 2016, ss 42, 43(3), and 97; US-UK Agreement (n 94) arts 1(11), 4(5) and 5(3); Designation Regulations (n 90), *Explanatory Memorandum* [7.7]. See also IPA 2016, s 261.

[243] See eg *Berger* (n 3) 57–63; *Zakharov v Russia* (2016) 63 EHRR 17 (GC) [168]–[169].

[244] Data Retention and Investigatory Powers Act 2014, s 4; Anderson (n 236) [6.95]–[6.99].

[245] 18 USC § 2510–2523. See eg *Dahda* (n 130).

[246] See Anderson (n 236) [8.43] and [13.35] [13.44]; Scott (n 239) 59–104.

[247] IPA 2016, s 56; Anderson (n 236) [9.16]–[9.18]. But see also *R v P* (n 185).

process.[248] The US-UK Agreement does, however, impose some restrictions, including by allowing only targeted, rather than 'bulk', data requests.[249]

Ultimately, it is beyond the scope of this thesis to determine the extent to which the UK's increased intercept ability undermines digital privacy rights. The combability of these intercept powers with Article 8 generally is an extensive and developing topic.[250] The IPA and predecessor legislation have been repeatedly challenged recently in European courts,[251] and a decision of the Grand Chamber of the ECtHR is pending.[252] These powers nonetheless serve as a potential caveat against the otherwise broadly rights-enhancing nature of the CLOUD Act regime for UK persons.

2.5.4 Reciprocal US requests for UK persons' data raise minor concerns

UK persons are relatively more exposed to US CLOUD Act regime requests than US persons in the equivalent scenario.[253] The US-UK Agreement is only quasi-reciprocal: while the UK is prohibited from targeting US persons at all times, the US is only prohibited from targeting UK persons when they are 'located in [UK] territory'.[254] This distinction, which arises from EU law,[255] should not be presumed immaterial. It is US policy to track

---

[248] Woods (n 154) 661; Paddy McGuinness, UK Deputy National Security Adviser, 'Written Testimony' (Judicial Sub-Committee on Crime and terrorism, US Senate, 10 May 2017). See also Daskal, 'Correcting the Record' (n 131).

[249] US-UK Agreement (n 94) art 4(5).

[250] See eg *Human Rights Watch* (n 4); *Tele2 Sverige AB v Post-och telestyrelsen* [2017] QB 771 (CJEU); *Big Brother Watch v United Kingdom* App no 5817/13 (ECtHR, 13 September 2018); *R (National Council for Civil Liberties) v Secretary of State for the Home Dept* [2019] EWHC 2057 (Admin), [2019] 1 WLR 243.

[251] ibid.

[252] See ECtHR, 'Grand Chamber hearing on complaints about surveillance systems in the case of Big Brother Watch and Others v. the United Kingdom' (ECHR 258 (2019), 10 July 2019).

[253] Compare text to nn 142–146.

[254] US-UK Agreement (n 94), arts 1(12) and 4(3). See also Jennifer Daskal and Peter Swire, 'The U.K.-U.S. CLOUD Act Agreement Is Finally Here, Containing New Safeguards' (*LawFare*, 8 October 2019) <www.lawfareblog.com/uk-us-cloud-act-agreement-finally-here-containing-new-safeguards> accessed 31 July 2020; Christakis '21' (n 90) III.1.

[255] Foreign and Commonwealth Office [**FCO**], *Explanatory Memorandum to the Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United*

targets and 'lure' them across borders.[256] The US has also historically engaged in analogous 'evidence laundering' practices.[257] The prospect that the US would adopt similar tactics to obtain a UK persons' data is therefore far from fanciful.

On the other hand, UK persons now benefit from additional protections when the US seeks their data under the SCA—whether or not this request is also made under the US-UK Agreement.[258] The CLOUD Act introduced an new enhanced comity test into the SCA enabling service providers to object to a US SCA request for a non-US person's data where 'disclosure would create a material risk that the provider would violate the laws of' a CLOUD Act regime country.[259] This should bring some comfort to UK persons.[260]

2.6 Third Country Nationals' (TCNs') Digital Privacy Rights, Already Limited Under MLA, Are Further Undermined By the CLOUD Act Regime

2.6.1 Overview

TCNs' digital privacy rights are protected even less than either US or UK persons under US-UK MLA. While different aspects of this MLA process favour one or other of the two countries' nationals, TCNs always lose out.

This continues under the CLOUD Act regime. Additionally, while the impact of UK requests under COPOA for TCNs is finely balanced, TCNs are overwhelmingly worse off when implicated by US CLOUD Act regime requests. This regime enhances protections for US and UK nationals precisely because each now benefits from the full application of the constitutional rights mechanisms of their own state. In contrast, TCNs

---

States of America on Access to Electronic Data for the Purpose of Countering Serious Crime (2019) [14]. See also Christakis, '21' (n 90) III.1.

[256] Prabhu, Berrang, and Dickey (n 72) 180.

[257] Boister (n 1) 331 (citing *R v Governor of Pentonville Prison, ex parte Chinoy* [1992] 1 All ER 317 (QB)).

[258] See Christakis '21' (n 90) III.2.

[259] CLOUD Act, § 130(c) (incorporated as 18 USC § 2703(h)). See also Schwartz (n 98) 1715.

[260] See Jennifer Daskal, '*Microsoft Ireland*, CLOUD Act, and International Law-Making 2.0' (2018) 71 Stan L Rev Online 9, 11–13. But see also Schwartz (n 98) 1715; Abraha (n 102) 17.

receive the burden of each state's laws, through the expanded enforcement jurisdiction the CLOUD Act regime facilitates, but none of the benefits their constitutional rights mechanisms provide. Moreover, the safeguards the US-UK Agreement purports to extend to TCNs appear illusory.

2.6.2 US-UK MLA does not protect TCNs' digital privacy rights

As set out above, the US and UK provide relatively reduced protections during MLA compared with equivalent domestic processes.[261] However, while US and UK nationals will, at varying stages, receive the benefits extended by the Fourth Amendment and Article 8, respectively,[262] these are always denied to TCNs, leaving them the worst-off of these three classes at all points.

Consider an MLA request from the US for a TCN's data held by a UK service provider. Even if a TCN were aware of this,[263] a preliminary challenge in the US would almost certainly fail, not least because Fourth Amendment grounds would be unavailable.[264] While a TCN would have standing to challenge the UK's subsequent steps—evaluating and executing the request, and then transmitting the resulting data—such applications have little chance of success.[265] Claims based on Article 8 would be prohibited.[266] Most significantly, when facing US criminal proceedings, a TCN would be barred from even arguing for one of the narrow exceptions to the 'international silver platter' doctrine'.[267]

---

[261] n 2.

[262] See eg text to n 51 and 158.

[263] See US-UK MLAT (n 19) art 7(1). See also nn 20 and 164.

[264] See *Verdugo-Urquidez* (n 134) 265–275; text to nn 12–26.

[265] Text to 27–57.

[266] *Human Rights Watch* (n 4) [55]; *Akarcay* (n 4) [35]–[36]. See also text to 51–57.

[267] *Fantin* (n 203).

The reciprocal scenario, when the UK is the requesting state, is also restrictive.[268] Exclusion of evidence remains available in principle, regardless of nationality or geography, under s 78 of PACE.[269] UK courts have treated s 78 as providing equivalent protections to Article 6 of the ECHR,[270] under which (in combination with Article 8) evidence obtained in breach of digital privacy rights may face exclusion.[271] However, the UK has upheld privacy protections relatively reluctantly.[272] The ECtHR has disagreed with multiple restrictive UK interpretations of Article 8 in the law enforcement context.[273] The mere fact a defendant is within the UK's jurisdiction for the purposes of the ECHR is therefore material, because it provides them with clear 'European supervision' through the ECtHR.[274] Under UK law, however, TCNs are always outside the UK's ECHR jurisdiction during MLA for Article 8 purposes.[275] This is equally true whether or not the TCN is from another ECHR member state or outside the '*espace juridique*' (legal space) of the ECHR altogether.[276]

2.6.3 The CLOUD Act regime further undermines TCNs' digital privacy rights

Unlike US and UK persons, TCNs' digital privacy rights will be even further reduced under the CLOUD Act regime, at least for US requests. The continued denial of Fourth Amendment protections for TCNs, along with the possibility the US may circumvent

[268] Text to nn 154–196.

[269] See eg *R v Okafor* (1994) 99 Cr App R 97 (EWCA).

[270] *R v P* (n 185) 161–162.

[271] See nn 185–187.

[272] Dickson (n 57) 228 See also eg *Sutherland v Her Majesty's Advocate (Scotland)* [2020] UKSC 32.

[273] See eg *Gillan and Quinton v UK* (2010) 50 EHRR 45; *Beghal v UK* (2019) 69 EHRR 28.

[274] *Mosley v United Kingdom* (2011) 53 EHRR 1011 [107].

[275] *Human Rights Watch* (n 4) [55].

[276] ibid.

ovstatutory protections and the absence of any genuine safeguards provided by the US-UK Agreement, leave TCNs in an unenviable position.

A preliminary question is again the methods the US could use to issue CLOUD Act regime requests.[277] While the Fourth Amendment would at least require US CLOUD Act regime requests targeting US persons to be reasonable,[278] it would not apply at all under *Verdugo-Urquidez* to requests targeting TCNs.[279] Professor Albert Gidari considers that the US therefore may be able to request non-US national's data from UK service providers using 'any number of lesser forms of legal process'.[280] As set out above, this may be consistent with the US-UK Agreement and US law, particularly as TCNs lack Fourth Amendment protections.[281] Regardless, even if requests are made exclusively under the SCA or Wiretap Act, the combination of the absence of any exclusionary remedies under these statutes and the removal of the (albeit limited) oversight of UK courts would represent a significant reduction in TCN's rights compared with MLA.

Neither of the two safeguards provided to TCNs by the US-UK Agreement displaces this conclusion.[282] The first requires a requesting state to notify 'the appropriate authorities in the third country where the person is located',[283] although not the target TCN.[284] This is vague,[285] potentially permitting notification to be delayed until after data

[277] See US-UK Agreement (n 94), arts 1(1) and 5(7)–(8). See also arts 5(1) and 10(2).

[278] *In re Terrorist Bombings* (n 78) 167–173; *Stokes* (n 72) 891–893.

[279] *Verdugo-Urquidez* (n 134) 265–275.

[280] Albert Gidari, 'More Questions' (n 138).

[281] Text to nn 133–138. See also *Verdugo-Urquidez* (n 134) 265–275.

[282] US-UK Agreement (n 94) arts 5(10)–(12).

[283] ibid art 5(10).

[284] See Christakis '21' (n 90) III.9.

[285] ibid III.6; Albert Gidari, 'The Big Interception Flaw in the US-UK CLOUD Act Agreement' (*The Center for Internet and Society*, 18 October 2019) <http://cyberlaw.stanford.edu/blog/2019/10/big-interception-flaw-us-uk-cloud-act-agreement> accessed 31 July 2020; Abraha (n 102) 22.

has been obtained.[286] It provides no mechanism for third countries to object at all,[287] let alone to an independent judicial body.[288] The requesting state may also avoid notification at its discretion where it 'considers that notification would be detrimental to operational or national security, impede the conduct of an investigation, or imperil human rights'.[289] There is a real risk that such broad exceptions 'become the rule'.[290]

The other safeguard is the ability of a service provider to 'raise specific objections when it has reasonable belief that the Agreement may not properly be invoked with regard to the Order'.[291] Objections are initially raised with the requesting state and then, if not resolved, may be escalated to the provider's own state.[292] The two states 'may confer in an effort to resolve any such objections', with the provider's own state having the final say.[293] Giving the provider's own state the ultimate determination is welcome but may well occur only rarely.[294] Service providers will be driven by commercial interests.[295] These may differ from their customers' interests, particularly where—as here—the target

[286] Gidari 'Big Interception Flaw' (n 285).

[287] Christakis '21' (n 90) Chart 1, Comment 7.

[288] Gidari 'Big Interception Flaw' (n 285). Compare Jennifer Daskal and Peter Swire, 'The US-UK CLOUD Act Agreement is Finally Here, Containing New Safeguards' (*JustSecurity*, 8 October 2019) <www.justsecurity.org/66507/the-uk-us-cloud-act-agreement-is-finally-here-containing-new-safeguards/> accessed 31 July 2020.

[289] US-UK Agreement (n 94) art 5(10). See Gidari 'Big Interception Flaw' (n 285); Abraha (n 285) 22.

[290] See Christakis '21' (n 90) III.6.

[291] US-UK Agreement (n 94) art 5(11).

[292] ibid art 5(11).

[293] ibid arts 5(11)–(12).

[294] See Daskal and Swire (n 288).

[295] See Els de Busser, 'The Digital Unfitness of Mutual Legal Assistance' (2017) 28 Sec and Human Rts 161 171–172; Andrew Keane Woods, 'Litigating Data Sovereignty' (2018) 28 Yale L J 328, 366 n225; Marco Stefan and Gloria González Fuster, 'Cross-border Access to Electronic Data through Judicial Cooperation in Criminal Matters' (CEPS Paper No 2018-07, November 2018, updated May 2019) vii and 37–40; Stanislaw Tosza, 'Mutual recognition by private actors in criminal justice? Service providers as gatekeepers of data and human rights obligations' (2020) CMLR (forthcoming) 20.

customer is a TCN and the provider is UK-based.[296] Providers may also 'face continuing government pressure to cooperate'.[297]

In any event, the US-UK Agreement implies that objections must arise from the law of the requesting state,[298] yet UK service providers may be unfamiliar with US law,[299] particularly the complexities of the CLOUD Act regime.[300] The other potential source of objections is the US-UK Agreement's reference to the US-EU 'Umbrella Agreement', regulating trans-Atlantic law enforcement data transfers.[301] However, this does not protect TCNs.[302] Similarly, even if requests are made under the SCA, its new comity defence, referred to above,[303] likely protects only UK nationals here.[304] Finally, while TCNs at least theoretically may have had remedies against a requested state improperly disclosing their data during MLA, their remedies against providers in this context are unclear.[305]

Whether TCNs targeted by CLOUD Act regime requests from the UK, at least for stored data, are worse off than under MLA is more nuanced. Unlike the ambiguity in the US,[306] UK requests should now be dealt with exclusively under COPOA; the legality of

---

[296] Daskal, 'Opening Salvo' (n 94) 339. See Tosza (n 295) 18.

[297] Jonathan Hafetz, 'The Possibilities and Limits of Corporations as Privacy Protectors in the Digital Age' in David Cole, Feredico Fabbrini and Stephen Schulhofer (eds), *Surveillance, Privacy and Trans-Atlantic Relations* (Hart Publishing 2019) 111. See also Tosza (n 295) 17–18.

[298] See US-UK Agreement (n 94) arts 1(11), 3, 5(1)–(2), 8(1)–(2), 10(1)–(2) and (5).

[299] Shelli Gimelstein, *Storm on the Horizon: How the U.S. CLOUD Act May Interact with Foreign Access to Evidence and Data Localization Laws* (*Data Analyst*, 2018) 6–7; Daskal, 'Opening Salvo' (n 94) 338–339.

[300] Christakis '21' (n 90) III.3

[301] US-UK Agreement (n 94) art 9(1); Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences [2016] OJ L 336/3.

[302] ibid art 4. See Judicial Redress Act of 2015 - Attorney General Designations 82 Fed Reg 7860 (23 January 2017); Judicial Redress Act of 2015 - Attorney General Designations 84 Fed Reg 3493 (12 February 2019) (US).

[303] Text to nn 258–260.

[304] 18 USC 2703(h). See Abraha (n 102) 17. Compare Daskal, 'Privacy and Security' (n 101) 1049–1050.

[305] See Tosza (n 295) 17–18.

[306] Text to nn 277–281 .

any lesser forms of legal process would be doubtful.[307] Overall, TCNs appear to receive similar (limited) digital privacy rights as before: COPOA provides protections comparable to the SCA and, as before, an exclusion remedy remains potentially available.[308] However, neither under MLA nor the CLOUD Act regime will TCNs be permitted to rely on Article 8, severely limiting their digital privacy rights.[309]

2.7 Conclusion

Chapter 2 confirms the continuing importance of concerns that MLA provides insufficient protection for the constitutional rights of implicated persons.[310] Human rights commonly fall through the gaps between the US and UK's legal systems during MLA,[311] contrary to claims outlined in Chapter 1 that MLA provides 'double protection' for rights.[312] These protection gaps under MLA apply with differing respects in relation to all three classes of persons. Chapter 2 also shows that for US and UK persons the shift from MLA to the CLOUD Act regime appears largely rights-enhancing. However, this analysis nonetheless undermines the US and UK's claim that the regime improves cross-border data access while 'respecting privacy and enhancing civil liberties' overall.[313] The third class of persons analysed—TCNs—already received the fewest protections for digital privacy rights under MLA. They will receive even fewer under the CLOUD Act regime. Overall, TCNs' digital privacy rights continue to be overlooked, leaving significant protection gaps.

---

[307] See generally COPOA 2019, *Explanatory Notes*. See also *Attorney General v De Keyser's Royal Hotel* [1920] AC 508 (HOL) 575; *R (Miller) v Secretary of State for Exiting the European Union* [2017] UKSC 5, [2018] AC 61 [55]–[56].

[308] PACE 1984, s 78.

[309] Text to nn 51–57.

[310] See eg Gane and Mackeral (n 23); Currie, 'Human Rights' (n 7) 171–177.

[311] Zeegers (n 1) 133–137; Tilman Altwicker, 'Transnationalizing Rights: International Human Rights Law in Cross-Border Contexts' (2018) 29 EJIL 581, 587. See also Currie, 'Human Rights' (n 7) 165–167.

[312] Lawrence Siry, 'Cloudy days ahead: Cross-border evidence collection and its impact on the rights of EU citizens' (2019) 10 NJECL 227, 232 and 250. See also Gane and Mackeral (n 23) 118–119.

[313] DOJ (n 98).

CHAPTER 3

3.1 Introduction

Chapter 3 addresses why and how US and UK law should be developed to fill the protection gap that exists for TCN's digital privacy rights under the CLOUD Act regime. It argues that it would be justified and proportionate to extend to TCNs the recognition and protection of both the Fourth Amendment of the US Constitution and Article 8 of the ECHR in the context of the CLOUD Act regime.

This Chapter first outlines why the protection gaps for TCNs' digital privacy rights are significant, both for TCNs themselves as well as the US and UK. It explains that extending digital privacy rights to TCNs would support the underlying aims of the CLOUD Act regime and be readily achievable in practice. It then considers how each of Fourth Amendment and Article 8 jurisprudence can and should be extended to fill these gaps. It argues that these developments would be consistent with long-term trends towards extraterritoriality in each jurisdiction and justified on policy grounds.

3.2 The Protection Gaps for TCNs' Digital Privacy Rights Under the CLOUD Act Regime Are Significant

3.2.1 TCNs are Exposed due to these protection gaps

As Chapter 2 explained, although the CLOUD Act regime enhances the digital privacy rights protections for the US and UK's own nationals, it undermines TCNs' rights, which already received insufficient protection under MLA. TCNs may be directly targeted,[1] yet have no meaningful ability to obtain relief for breaches of their rights under either the Fourth Amendment or Article 8 due to specific limitations—one nationality-based, the other territorial—imposed under existing authorities.

[1] See Foreign and Commonwealth Office, 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 (CP 178, 3 October 2019) [**US-UK Agreement**] art 5(10).

The Fourth Amendment imposes a *nationality-based* limitation, effectively prohibiting TCN's ability to use the Fourth Amendment to protect digital privacy rights against US misconduct. Unlike the UK / ECHR position, US jurisprudence readily accepts that the Fourth Amendment applies extraterritorially to constrain US law enforcement overseas.[2] However, *Verdugo-Urquidez* is commonly applied as authority that the Fourth Amendment's protections do not extend to TCNs until they form 'substantial connections' with the US.[3] The Fourth Amendment normally 'has no application' to non-US nationals, whether the search at issue is 'extraterritorial' or not.[4] This leaves TCNs typically unable to exclude electronic data obtained through potentially unlawful US law enforcement searches.[5] The same approach is expected to apply under the CLOUD Act regime.[6]

In contrast, Article 8, like all ECHR rights, applies regardless of nationality.[7] Article 1 of the ECHR requires the UK and all ECHR member states to 'secure to everyone within their jurisdiction the rights and freedoms' of the ECHR. In jurisprudence followed by the UK,[8] the ECtHR has interpreted Article 1 as imposing a 'primarily territorial' limit

[2] *Reid v Covert* 354 US 1, 5–6 (1957); *US v Conroy* 589 F2d 1258, 1264 (5th Cir 1979); *US v Verdugo-Urquidez* 494 US 259, 277 (1990) (Kennedy J concurring). See also eg *US v Stokes* 726 F3d 880, 890–891 (7th Cir 2013); *US v Emmanuel* 565 F3d 1324, 1330 (11th Cir 2009).

[3] See eg *Emmanuel* (n 2) 1331–1332.

[4] *Verdugo-Urquidez* (n 2) 275. Compare *US v Gorshkov* 2001 WL 1024026, No CR00-550C *3 (WD Wash 23 May 2001); *Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp* 829 F3d 197, 220–221 (2d Cir 2016).

[5] See eg *Gorshkov* (n 4); *US v Loera* 333 F Supp 3d 172, 181–182 (EDNY 2018). See also Jennifer Daskal, 'The Un-territoriality of data' (2015) 125 Yale L J 326, 339–340.

[6] Peter Swire and Justin Hemmings, 'Overcoming Constitutional Objections to the CLOUD Act' (American Constitution Society, Issue Brief, February 2020) 7–8. See also Paul M Schwartz, 'Legal Access to the Global Cloud' (2018) 118 Colum L Rev 1681, 1712.

[7] See ECHR, art 1; Francesca Bignami and Giorgio Resta, 'Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance' in Eyel Benvenisti & Georg Nolte (eds) *Community Interests Across International Law* (OUP 2018) 375.

[8] *Smith v Ministry of Defence* [2013] UKSC 41, [2014] AC 52 [27]–[55]; *R (Al-Saadoon) v Secretary of State for Defence* [2015] EWHC 715 (Admin), [2016] EWCA Civ 811 [106].

on ECHR obligations,[9] and extending extraterritorially only exceptionally.[10] Two circumstances have been recognised to date.[11] The ECtHR has never considered their application in the digital sphere but UK courts have, holding in *Human Rights Watch* that the UK owes no Article 8 obligations to persons outside UK territory when intercepting their data.[12] This approach is echoed in other UK judgments recognising extraterritorial ECHR jurisdiction only where the UK has physical power or control over an overseas territory or person.[13] Therefore, even if the UK's own CLOUD Act regime acts fall within the 'extraterritorial' scope of Article 1 for UK persons, as discussed in Chapter 2,[14] UK authorities nonetheless bar TCNs from raising Article 8 claims.

3.2.2 These protection gaps undermine the US and UK's own aims

While the protection gaps identified above are undoubtedly important for TCNs themselves, they should be considered equally significant to the US and UK. As set out previously, the US and UK claim that the CLOUD Act regime—which operates through the local laws of its member states[15]—'respect[s] privacy and enhance[s] civil liberties'.[16] It claims to provide an 'efficient, effective, data protection-compatible and privacy-

[9] See eg *Bankovic v Belgium* (2001) 44 EHRR SE5 [59]–[61]; *Al-Skeini v UK* (2011) 53 EHRR 18 (GC) [131].

[10] *Al-Skeini* (n 9) [131]–[132].

[11] ibid [133]–[140]. See also [141]–[142].

[12] *Human Rights Watch Inc v Secretary of State for the Foreign and Commonwealth Office* [2016] UKIPTrib 15_165_CH [49]–[62]. See also Lea Raible, '*Human Rights Watch v Secretary of State for the Foreign and Commonwealth Office*: Victim Status, Extraterritoriality and the Search for Principled Reasoning' (2017) 80 MLR 510, 518.

[13] *R (Zagorski) v Secretary of State for Business, Innovation and Skills* [2010] EWHC 3110, [2011] HRLR 6 [57]; *R (Sandiford) v Secretary of State for Foreign and Commonwealth Affairs* [2014] UKSC 44, [2014] 1 WLR 2697 [21]–[34]; *R (Akarcay) v Chief Constable of the West Yorkshire Police* [2017] EWHC 159 (Admin) [7]–[8] and [35]–[36].

[14] See *Al-Skeini* (n 9) [135].

[15] US-UK Agreement (n 1) arts 2(1), 3, 5(1)–(2), 6(2)–(3), 8(1)–(2), 9(2), and 10(1)–(2), (5)–(6), and (10).

[16] DOJ, 'U.S. and UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online' (3 October 2019) <www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists>.

protective means' of accessing overseas data.[17] However, neither US nor UK law as currently applied respects TCN's digital privacy rights, yet they may be implicated by requests as well as directly targeted.[18] For the CLOUD Act regime to be implemented consistently with the US and UK's aims, a shift in thinking regarding the scope of the Fourth Amendment and Article 8 is therefore required.

The US and UK also have a strong interest in maintaining a free and open internet and opposing 'data localisation' and 'balkanisation', by which states mandate local storage of their own nationals' data and limit outside access.[19] Avoiding these developments is an aim of the CLOUD Act regime itself.[20] This would be furthered if the regime respected TCNs' digital privacy rights on an equal footing with the rights of its own members' nationals, because other states would then not be as incentivised to localise their data to protect it from US and UK requests.[21] These states could 'teach by doing',[22] by extending protections to TCNs in this context. This would also increase the attractiveness of the regime for other rights-respecting countries, who may otherwise fear that improper CLOUD Act regime conduct against TCNs may be attributable to them.[23] The US in particular has the opportunity to set the global approach in cross-border data access, given the current dominance of US service providers.[24] As it currently exists, however, the

[17] US-UK Agreement (n 1) art 2(2).

[18] ibid art 5(10).

[19] Daskal, 'Un-territoriality' (n 5), 333–334 and 392–393.

[20] US-UK Agreement (n 1), preamble and art 2(3)(c). See also Peter Swire and Justin D Hemmings, 'Mutual Legal Assistance In an Era of Globalized Communications: The Analogy To the Visa Waiver Program (2017) 71 NYU Ann Surv of American L 687, 710–714 and 728; Andrew Keane Woods, 'Litigating Data Sovereignty' (2018) 28 Yale L J 328, 400–401.

[21] See Daskal, 'Un-Territoriality' (n 5) 333–334 and 393; Paul M Schwartz, 'Legal Access to the Global Cloud' (2018) 118 Colum L Rev 1681, 1706–1707. See also Woods (n 19) 400–401.

[22] Amy E Pope, 'Lawlessness Breeds Lawlessness: A Case for Applying the Fourth Amendment to Extraterritorial Searches' (2013) 65 Fla L Rev 1917, 1922. See also Daskal, 'Law Enforcement Access'(n 24) 500.

[23] See Patricia L Bellia, 'Chasing Bits Across Borders' (2001) U Chi Legal F 35, 83–99.

[24] Peter Swire and DeBrae Kennedy-Mayo, 'How Both the EU and the U.S. Are Stricter than Each Other for the Privacy of Government Requests for Information' (2017) 66 Emory LJ 617, 664. See also Jennifer

regime's failure to respect TCNs' rights incentivises precisely the conduct that the US and UK hope to avoid.[25]

3.2.3 Filling these gaps by developing constitutional rights is appropriate and achievable

This thesis argues that the best method for securing TCNs' digital privacy rights in the context of the CLOUD Act regime is by extending the protections of the Fourth Amendment and Article 8. As set out in Chapter 1, these constitutional rights mechanisms provide the primary protection for digital privacy rights in the criminal context in each jurisdiction. This would ensure TCNs receive equal treatment from a constitutional perspective with US and UK nationals here.[26]

Alternative methods would be insufficient. Enhanced legislative protections, while welcome,[27] may be surpassed by subsequent judicial constitutional developments,[28] leaving those protected solely by legislation with inferior rights.[29] It has also been suggested that the ability to target TCNs should be removed altogether.[30] However, crime is increasingly transnational,[31] particularly when investigating terrorism and similar investigations that the CLOUD Act regime is intended to facilitate.[32] Prohibiting requests

---

Daskal, 'Privacy and Security across Borders' (2018–2019) 128 Yale LJ F 1029, 1050–1051; Jennifer Daskal, 'Law Enforcement Access to Data across Borders: The Evolving Security and Rights Issues (2016) 8 J Natl Sec L & Poly 473, 500; Schwartz (n 25) 1684.

[25] ibid.

[26] See also Woods (n 20) 395–399.

[27] Orin S Kerr, 'Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law' (2003) 54 Hastings LJ 805.

[28] See eg *US v Warshak* 631 F3d 266, 288 (6th Cir 2010); *Carpenter v US* 583 US __, __, 138 S Ct 2206, 2219–2222 (2018).

[29] See eg *US v Fantin* 130 F Supp 2d 385, 391 (WDNY 2000).

[30] Albert Gidari, 'Can the US-UK CLOUD Act Agreement Be Fixed?' (*The Center for Internet and Society*, 18 November 2019) <http://cyberlaw.stanford.edu/blog/2019/11/can-us-uk-cloud-act-agreement-be-fixed> accessed 31 July 2020;

[31] Neil Boister, *An Introduction to Transnational Criminal Law* (2nd edn, OUP 2018) 3–9.

[32] DOJ, *Promoting Public Safety, Privacy and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act* (White Paper, April 2019) [**DOJ, *White Paper***] 2 and 10; FCO, *Explanatory Memorandum to the Agreement between the Government of the United Kingdom of Great Britain and*

on the basis of nationality or location would therefore severely detract from the regime's claimed benefits. It would also be impractical, as often the nationality or location of a target is unknown.[33] Finally, it would again be insufficient, as TCNs' data would still be incidentally collected in circumstances implicating their rights.[34]

Extending these protections would also be achievable. While such recognition is principally a matter for the applicable courts, to which this Chapter's analysis speaks, it may be relatively simple to practically implement this through amending the US-UK Agreement itself.[35] Alternatively, this change could be effected voluntarily by each state, simply by not opposing claims in litigation under these rights mechanisms by TCNs and/or actively supporting them.[36]

3.3 Extending Fourth Amendment Rights to TCNs Under the CLOUD Act Regime

3.3.1 Overview

The US Supreme Court's approach to the extraterritorial application of constitutional rights is more nuanced and potentially generous to TCNs than *Verdugo-Urquidez* and its application by lower courts initially indicates.[37] Properly interpreted, the Supreme Court case law evidences an overall trend towards increased extraterritoriality of such rights, including for TCNs. Recognition of TCNs' digital privacy rights in this context would be an appropriate incremental step in Fourth Amendment jurisprudence.

Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime (2019) [**FCO, *Explanatory Memorandum***] [1].

[33] Orin S Kerr, 'The Fourth Amendment and the Global Internet' (2015) 67 Stanford L Rev 285, 303; Daskal, 'Un-territoriality' (n 5) 349.

[34] See Daskal, 'Privacy and Security' (n 50) 1048.

[35] US-UK Agreement (n 1) art 14.

[36] See eg *Big Brother Watch v UK* App no 58170/13 (ECtHR, 13 September 2018) [271]; *US v Ross* 963 F3d 1056, 1065–1066 (11th Cir 2020).

[37] See also Jennifer Daskal, 'Transnational seizures: the constitution and criminal procedure abroad' in Federico Fabbrini and Vicki C Jackson (eds), *Constitutionalism across borders in the struggle against terrorism* (Elgar 2016) 192.

3.3.2 There is a trend towards extraterritoriality in US Constitutional law

As set out in Chapter 2, most US analyses of TCNs' digital privacy rights simply applies *Verdugo-Urquidez*.[38] It is therefore appropriate to begin—although not end—by summarising this decision. The defendant was a foreigner who had been forcefully brought to the US just days before US law enforcement searched his house in Mexico.[39] The court held that the defendant was not entitled to seek suppression of the evidence gained from that search because he lacked Fourth Amendment rights.[40] The fact the defendant was in US territory when the extraterritorial search occurred was insufficient to trigger Fourth Amendment protections.[41] Instead, Rehnquist CJ, delivering the main judgment, held that aliens only 'receive constitutional protections when they have come within the territory of the United States and developed substantial connections with this country'.[42]

Rehnquist CJ's *Verdugo-Urquidez* judgment was a plurality opinion,[43] with Kennedy J providing the crucial fifth vote in a separate concurrence.[44] Kennedy J disagreed with aspects of the plurality's reasoning (summarised below), instead supporting the appeal on the narrow basis that 'adherence to the Fourth Amendment's warrant requirement' would be 'impracticable and anomalous' in the circumstances.[45] Professor Wayne LaFave, a leading Fourth Amendment scholar, has suggested that Kennedy J's reasoning is therefore '[t]he most that can be definitely concluded' from the case.[46] In any

---

[38] n 5.

[39] *Verdugo-Urquidez* (n 2) 272.

[40] ibid 274–275.

[41] ibid 271–272.

[42] ibid 271.

[43] ibid 261–275.

[44] ibid 275–278 (Kennedy J concurring).

[45] ibid 278 (Kennedy J concurring).

[46] *Search and Seizure: A Treatise on the Fourth Amendment* vol 1, § 1.8(h) (updated October 2019). See also Jacco Bomhoff, 'The Reach of Rights: "The Foreign" and "The Private" in Conflict-of-Laws, State-Action,

event, *Verdugo-Urquidez* was not the Supreme Court's last word on extraterritoriality of rights.[47] In 2008, the court issued *Boumediene v Bush*, rejecting a 'formalist' approach.[48] The majority judgment, also authored by Kennedy J, held instead that 'questions of extraterritoriality tun on objective factors and practical concerns, rather than formalism', and highlighted several factors favouring extraterritorial recognition of rights.[49]

Boumediene has ignited debates over whether TCNs (outside US territory) should be afforded the protection of particular US Constitutional rights,[50] including the Fourth Amendment.[51] Its precise impact on the precedent value of *Verdugo-Urquidez* remains unclear.[52] For example, in 2017 the Supreme Court declined to consider a TCN's Fourth Amendment claim, but noted that the question raised was 'sensitive and may have consequences that are far reaching.'[53] Although lower courts continue to regularly apply *Verdugo-Urquidez*,[54] the above context suggests that the bright-line rule against recognition of TCN's Fourth Amendment rights is not as firm as it first appears.

---

and Fundamental-Rights Cases With Foreign Elements' (2008) 71 L & Cont Probs 39, 45; Kerr (n 33) 292–294;

[47] *Zadvydas v Davis* 533 US 678, 693 (2001); *Boumediene v Bush* 553 US 723, 763–764 (2008); *Agency for Intl Devpt v Alliance for Open Society Intl Inc* 591 US __, 140 SCt 2082, 2086–2087 (2020). See also *Hernández v Mesa*, 582 US __, __, 137 S Ct 2003, 2007 (2017).

[48] *Boumediene* (n 47) 763.

[49] ibid 764. See also 764–766.

[50] See eg *US v Wanigasinghe* 545 F3d 595, 597 (7th Cir 2008); *Hamad v Gates* 732 F3d 990, 1005 (9th Cir 2013); *Hernández* (n 47) 265; *US v Hayes* 99 F Supp 3d 409, 413–415 (SDNY 2015); *Ali v Trump* 959 F3d 364, 368 (DCC 2020).

[51] See eg *US v Ali* 71 MJ 256, 277–278 (CAAF 2012) (Baker CJ concurring in part); *Hedges v Obama* 724 F3d 170, 194 n140 (2d Cir 2013); *Ai Otro Lado Inc v McAleenan* 394 F Supp 3d 1168, 1221 (SD Cal 2019).

[52] Bomhoff (n 46) 46; Daskal, 'Transnational seizures' (n 37) 196–197; Margaret Kopel, 'Injustice at the Border: Application of the Constitution Abroad through the Conflict of Laws' (2019) 167 U Pa L Rev 1241, 1251 n79; Fatma E Marouf, 'Extraterritorial Rights in Border Enforcement' (2020) 77 Wash & Lee L Rev 751, 816–817. See also *Hernández v US* 757 F3d 249, 265 (5th Cir 2014).

[53] *Hernández* (n 47) 2007. See also *Hernández v Mesa* 589 US __, __, 140 S Ct 735, 754 (2020) (Breyer J dissenting).

[54] See eg *US v Olaniyi* 796 Fed Appx 601, 603 (11th Cir 2019). See also Daskal, 'Transnational seizures' (n 37) 196–197.

It is however necessary to acknowledge a very recent Supreme Court judgment, *Agency for International Development v Alliance for Open Society International Inc*.[55] Delivering the court's opinion in late June 2020, Kavanaugh J claimed that 'it is long settled as a matter of American constitutional law that foreign citizens outside U. S. territory do not possess rights under the U. S. Constitution'.[56] This was strongly criticised as a 'sweeping assertion' by Breyer J in a dissenting judgment,[57] and is also arguably *obiter dicta*.[58] Breyer J stated that the court has 'studiously avoided establishing an absolute rule' in this area.[59] At the time of writing, the significance of Kavanaugh J's judgment remains to be seen.[60]

3.3.3 Recognition of TCNs' Fourth Amendment rights here is justified under both Boumediene *and* Verdugo-Urquidez

Verdugo-Urquidez was based on 'unashamed' policy grounds.[61] These must now be read in light of the four factors recognised as relevant in extending rights extraterritorially outlined in *Boumediene*, as recently interpreted by Breyer J.[62] All favour recognition of TCNs' Fourth Amendment rights here.

---

[55] *Agency for Intl Devpt* (n 47). See also *Dept of Homeland Security v Thuraissigiam* 591 US __, __, 140 S Ct 1959, 1981 and 1988 (2020).

[56] *Agency for Intl Devpt* (n 47) 2086–2087.

[57] ibid 2099–2100 (Breyer J dissenting).

[58] ibid 2099 (Breyer J dissenting).

[59] ibid.

[60] See Amanda L Tyler, 'Thuraissigiam and the Future of the Suspension Clause' (*LawFare*, 2 July 2020) <www.lawfareblog.com/thuraissigiam-and-future-suspension-clause> accessed 31 July 2020.

[61] C Gane and 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' (1994) 4 Eur J Crime, Crim L & Crim Just 98, 109. For additional critiques, compare *Verdugo-Urquidez* (n 2) 265–273, with ibid 275–278 (Kennedy J concurring); 286–293 (Breyer J dissenting); Marko Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (2015) 56 Harvard Intl L J 81, 87–94.

[62] See *Boumediene* (47) 764–766 (cited in *Agency for Intl Devpt* (n 47) 2100 (Breyer J dissenting)).

One *Boumediene* factor is the extent to which extending rights would be feasible in the particular circumstances.[63] A second, related here, is the degree of US control over the extraterritorial area.[64] Both favour recognising TCN's Fourth Amendment rights in this context. US law enforcement can readily extend rights to the TCNs targeted or otherwise implicated by CLOUD Act regime requests and, indeed, will apply such rights when targeting potential US persons.[65] As set out in Chapter 2, the US is permitted to extend their enforcement jurisdiction over UK service providers, thus allowing them extensive control over this (virtual) territory.

Countervailing practical concerns in *Verdugo-Urquidez* do not apply.[66] The Supreme Court feared that extending the Fourth Amendment extraterritorially to TCNs 'would plunge them into a sea of uncertainty as to what might be reasonable' abroad,[67] potentially implicating 'differing and perhaps unascertainable conceptions of reasonableness and privacy'.[68] However, under the US-UK Agreement, US requests will be governed solely by US law.[69] Extending the Fourth Amendment's warrant requirement was seen as particularly problematic because a US warrant would be a 'dead letter' abroad.[70] However, under the CLOUD Act regime, it is no longer true that 'an American law enforcement officer would not be permitted under British law to waltz into a London

[63] *Boumediene* (n 47) 766 (cited in *Agency for Intl Devpt* (n 47) 2100 (Breyer J dissenting)).

[64] ibid.

[65] n 2.

[66] See *Verdugo-Urquidez* (n 2) 264 and 273–275 (Rehnquist CJ); 278 (Kennedy J concurring). See also Laura K Donohue, 'The Fourth Amendment in a Digital World' (2017) 71 NYU Ann Surv Am L 553, 564.

[67] *Verdugo-Urquidez* (n 2) 274.

[68] ibid 278 (Kennedy J concurring).

[69] US-UK Agreement (n 1) arts 3(2), 5(1), 5(2), 8(1), 10(2) and 10(5)).

[70] *Verdugo-Urquidez* (n 2) 274; 278 (Kennedy J concurring); 279 (Stevens J concurring); 297 (Blackmun J dissenting). See also *In re Terrorist Bombings of US Embassies in E Africa* 552 F3d 157, 167–173 (2d Cir 2008); *Stokes* (n 1) 891–893.

premises and execute [a] search authorized by the American magistrate judge';[71] this is the regime's precise aim (albeit the 'waltzing' will occur electronically).

A third *Boumediene* factor is the particular relationship of the TCNs to the US,[72] while the fourth and final is the nature of the constitutional protection sought.[73] The particular relationship here solely concerns TCNs implicated in US CLOUD Act regime requests. This is a clearly defined, limited relationship. The nature of the protection sought is equally constrained: extending Fourth Amendment protections over US requests will simply require US law enforcement to treat all data sought and obtained equally, both at the time of acquisition and in subsequent proceedings. It is undisputed that the US will extend Fourth Amendment protections to US persons' data in these circumstances.[74] Both Daskal and Professor Orin Kerr further argue that, where the nationality or location of the owner of data is unknown—as it often will be[75]—US law enforcement should presume it attracts Fourth Amendment protections.[76] Assuming this approach is adopted, it would not be onerous to do this for all regime data. Related concerns in *Verdugo-Urquidez* that compliance with the Fourth Amendment extraterritorially would be overly burdensome are therefore inapposite,[77] as are worries that US courts would be inundated with spurious arguments if Fourth Amendment protections applied to TCNs.[78] US courts regularly hear, and commonly dismiss, claims by TCNs despite *Verdugo-Urquidez* without difficulties.[79]

---

[71] *US v Vilar* Case No S3 05–CR–621 (KMK), 2007 WL 1075041 *52 (SDNY 4 April 2007).

[72] *Boumediene* (n 47) 766 (cited in *Agency for Intl Devpt* (n 47) 2100 (Breyer J dissenting)).

[73] ibid.

[74] Text to n 2.

[75] n 33.

[76] Kerr (n 46) 313–316; Daskal, 'Un-territoriality' (n 5) 383–386. See also *Verdugo-Urquidez* (n 2) 285 (Brennan J dissenting); *Boumediene* (n 47) 765; Pope 1939–1942.

[77] *Verdugo-Urquidez* (n 2) 274.

[78] ibid 274.

[79] See eg *Hernández* (n 47). See also Daskal, 'Transnational seizures' (n 37) 204–205.

Additionally, foreign policy factors, a policy area recognised as relevant to extraterritoriality analysis in *Verdugo-Urquidez*, also support recognition.[80] The specific concerns raised there—potentially 'deleterious consequences' for the US military—are inapplicable here, as the CLOUD Act regime is a tool for law enforcement.[81] However, the US's foreign policy aim of enhancing rights globally would be furthered by recognising Fourth Amendment protections over these particular TCN relationships.[82] As suggested above, this would set a rights-enhancing global approach for other nations to follow.[83] Additionally, extending protections will minimise potential 'diplomatic and legal complications' with TCNs' own nations.[84]

Finally, Rehnquist CJ concluded in *Verdugo-Urquidez* that any 'restrictions on searches and seizures which occur incident to [overseas] American action … must be imposed by the political branches through diplomatic understanding, treaty, or legislation.'[85] The US-UK Agreement may be exactly such a treaty. Although this argument was previously rejected in relation to a MLAT,[86] the CLOUD Act regime purports to be different. In addition to the general rights-enhancing claims its members make regarding the regime,[87] unlike typical MLATs,[88] the US-UK Agreement extensively

---

[80] *Verdugo-Urquidez* (n 2) 273–274. See also Peter Swire, Jesse Woo and Deven R Desai, 'The Important, Justifiable, and Constrained Role of Nationality in Foreign Intelligence Surveillance (Aegis Series Paper No 1901, Hoover Institution, 2019) 19. But see also *Verdugo-Urquidez* 291 (Brennan J dissenting); Daskal, 'Transnational seizures' (n 37) 205–206.

[81] US-UK Agreement (n 69) Preamble and art 2(1); Jennifer Daskal, 'The Opening Salvo: The CLOUD Act, e-Evidence Proposals, and EU–US Discussions Regarding Law Enforcement Access to Data across Borders' in Francesca Bignami (ed) *EU Law in Populist Times: Crises and Prospects* (CUP 2020) 335.

[82] See DOJ (n 16).

[83] Text to nn 24–22.

[84] *In re Terrorist Bombings* (n 70) 171 (citing *Vilar* (n 71) *52).

[85] *Verdugo-Urquidez* (n 2) 275.

[86] *US v Defritas* 701 F Supp 2d 297, 304 (EDNY 2010).

[87] DOJ (n 16).

[88] See Boister (n 31) 323; Robert J Currie, 'The protection of human rights in the suppression of transnational crime' in Neil Boister and Robert J Currie, *Routledge handbook of transnational criminal law* (Routledge, Taylor and Francis Group 2015) 39–40.

references privacy and other human rights throughout.[89] Its approval by Congress could thus be viewed as a deliberate restriction on overseas US search and seizure powers through the extension of TCN rights suggested here.

3.4 Recognising the 'Virtual Jurisdiction' of Article 8 over CLOUD Act regime Requests

3.4.1 Overview

Unlike the Fourth Amendment, ECHR protections discriminate not based on nationality but 'jurisdiction' which, in ECHR jurisprudence, is primarily territorial.[90] There is nonetheless a significant trend towards extraterritorial recognition of ECHR rights generally, as well as broad recognition that a reconceptualization of the ECtHR's two extraterritoriality models is warranted. Whatever particular new model is adopted for Article 8 must be one that treats TCNs impacted by CLOUD Act regime requests as within the UK's 'virtual jurisdiction' for the purposes of Articles 1 and 8.

3.4.2 There is a trend towards increased extraterritoriality of ECHR rights

There is a clear trend in ECtHR jurisprudence towards a 'more expansive approach' to extraterritorial jurisdiction under Article 1.[91] The 2011 ECtHR Grand Chamber judgment *Al-Skeini v United Kingdom* applied the ECHR to UK operations in Iraq,[92] taking a more expansive approach than before.[93] Subsequent cases appear to even further expand the

[89] US-UK Agreement (n 1), Preamble, art 2(1), 3(3), 8(1), 9, and 10(10).

[90] *Al-Skeini* (n 9) [131].

[91] Marko Milanovic, 'Jurisdiction and Responsibility: Trends in the Jurisprudence of the Strasbourg Court', in Anne van Aaken and Iulia Motoc (eds) *The European Convention on Human Rights and General International Law* (OUP 2018) 102. See also eg Bignami and Resta (n 7) 375; Eliza Watt, 'The Role of International Human Rights Law in the Protection of Online Privacy in the Age of Surveillance' in H. Rõigas and others (eds), *2017 9th International Conference on Cyber Conflict: Defending the Core* (2017) NATO CCD COE) 104.

[92] *Al-Skeini* (n 9).

[93] Compare *Bankovic* (n 9). See also Samantha Besson, 'The Extraterritoriality of the European Convention on Human Rights: Why Human Rights Depend on Jurisdiction and What Jurisdiction Amounts to' (2012) 25 Leiden J of Intl L 857.

ECHR's extraterritorial scope, although these largely deal with questions of jurisdiction over physical territory, such as military checkpoints on foreign territory.[94]

The ECtHR's expansive extraterritorial jurisdiction is also reflected in its cases in the digital sphere, although it has never clarified its approach to jurisdiction in this context.[95] In 2018, the ECtHR determined a claim against aspects of UK's intercept powers in *Big Brother Watch v UK*, including the compatibility of its 'bulk' intercept powers with Article 8.[96] As set out in Chapter 2, this was appealed to the Grand Chamber, the judgment of which is pending.[97] The UK did not object in *Big Brother Watch* to the jurisdiction of the applicants bringing Article 8 claims, although these included individuals based outside UK territory.[98] Two previous surveillance cases involving applicants outside the territory of the respondent state have also been decided by the ECtHR without extraterritoriality concerns being decisive.[99] The ECtHR could have, but did not, dismiss such claims on Article 1 grounds of its own volition.[100]

A considerable shortcoming of the ECtHR's expanded approach to jurisdiction is its failure to acknowledge when it is doing precisely that; it instead attempts to fit existing precedents within any new framework.[101] This has generated a 'patch-work' of differing

---

[94] Lea Raible, 'The Extraterritoriality of the ECHR: Why *Jaloud* and *Pisari* should be Read as Game Changers' [2016] Eur Hum Rts L Rev 161. See also eg Milanovic, 'Jurisdiction' (n 91) 99–103.

[95] Text to n 12.

[96] *Big Brother Watch* (n 36).

[97] See ECtHR, 'Grand Chamber hearing on complaints about surveillance systems in the case of Big Brother Watch and Others v. the United Kingdom' (ECHR 258 (2019), 10 July 2019).

[98] *Big Brother Watch* (n 36) [271] and Appendix.

[99] *Weber v Germany* (2008) 46 EHRR SE5 [66] and [72]; *Liberty v United Kingdom* (2009) 48 EHRR 1 [55]. See also Milanovic, 'Human Rights Treaties' (n 61) 127.

[100] See Holly Huxtable, 'E.T. Phone Home…They Know: The Extraterritorial Application of Human Rights Treaties in the Context of Foreign Surveillance' (2017) 28 Sec and Hum Rts 92, 94–95; Kathryn Wilson, 'The European Convention on Human Rights and the Investigatory Powers Tribunal: Rationalising a Law unto Itself?' (2020) 23 Trinity CL Rev 129, 145.

[101] See Marco Milanovic, '*Al-Skeini* and *Al-Jedda* in Strasbourg' (2012) 23 EJIL 121, 129 and 131.

case law.[102] Current ECtHR jurisprudence recognises two models for extraterritorial jurisdiction, commonly referred to as the 'spatial' and 'personal' models.[103] The spatial model applies where a state has 'effective control of an area outside [its] national territory'.[104] The personal model applies where a state's 'agents exert authority or control' over an individual.[105] The application of these two models in practice is, however, far from clear.[106] In *Al-Skeini*, delivering his final judgment, Bonello J famously called for the ECtHR to 'return to the drawing board' regarding jurisdiction.[107]

As a result, although there is a general trend towards expansive extraterritoriality, the confused approach of ECtHR case law has enabled UK courts to adopt the narrow interpretation to Articles 1 and 8 exemplified in *Human Rights Watch* and similar cases.[108] *Human Rights Watch* has been overwhelmingly criticised.[109] Commentators do however acknowledge that neither existing ECtHR extraterritoriality model appears appropriate for the digital world.[110] Law enforcement in one country may interfere with electronic data stored in a second, thus undermining the digital privacy rights of a person in a third country

---

[102] *Al-Skeini* (n 9) [5] (Bonello J concurring). See also Raible, '*Jaloud*' (94) 161; Milanovic, 'Jurisdiction' (n 91) 98; Huxtable (n 100) 102 and 112; Wilson (n 100) 144.

[103] See eg Raible, '*Jaloud*' (n 94) 163; Milanovic, 'Jurisdiction' (n 91) 97–99.

[104] *Al-Skeini* (n 9) [138].

[105] ibid [133]–[137].

[106] See Raible, '*Jaloud*' (n 94); Milanovic, 'Jurisdiction' (91) 97–103.

[107] *Al-Skeini* (n 9) [8] (Bonello J concurring). See also Huxtable (n 100) 107–112.

[108] nn 12–13.

[109] Marko Milanovic, 'UK Investigatory Powers Tribunal Rules that Non-UK Residents Have no Right to Privacy under the ECHR' (*EJIL:Talk!*, 18 May 2016) <www.ejiltalk.org/uk-investigatory-powers-tribunal-rules-that-non-uk-residents-have-no-right-to-privacy-under-the-echr/> accessed 31 July 2020; Raible, '*Human Rights Watch*' (n 12); Huxtable (n 100); Helen McDermott, 'Application of the International Human Rights Law Framework in Cyber Space' in Dapo Akande and others, *Human Rights and 21st Century Challenges* (OUP 2020) 203–204; Wilson (n 100) 144–146. See also Watt (n 91) 99–100; Tilman Altwicker, 'Transnationalizing Rights: International Human Rights Law in Cross-Border Contexts' (2018) 29 EJIL 581, 587; Bignami and Resta (n 7) 377; Cedric MJ Ryngaert and Nico ANM van Eijk, 'International cooperation by (European) security and intelligence services: reviewing the creation of a joint database in light of data protection guarantees' (2019) 9 Intl Data Privacy L 61, 67; Kristian P Humble, 'International law, surveillance and the protection of privacy' (2020) Int J of Hum Rts (forthcoming) 10.

[110] See eg Milanovic, 'UK Investigatory Powers Tribunal' (n 109); Raible '*Human Rights Watch*' (n 12) 518; Huxtable (n 100) 95–96; McDermott (n 109) 203.

entirely.[111] The existing models simply do not accommodate such interferences, whether for law enforcement or other intelligence purposes, in which there is a 'disconnect between the location of the individual and the location of the interference' with their privacy.[112]

This is particularly problematic for requests for TCNs' data under the CLOUD Act regime. TCNs are assumed to always be in a third country: not the US, nor the UK. In those scenarios, the spatial model is unlikely to apply. This extends jurisdiction to territories in which the UK has effective control. Even if the UK were considered to have effective control over, for example, the physical location where US service provider was based, the TCN is not there; they are in a third country.[113] Yet the spatial model's application typically requires control over the very territory in which the affected person is based.[114]

The personal model suffers a similar fate. One circumstance triggering its application is where the state acting extraterritorially is exercising certain 'public powers' normally exercised by the other state in which it is acting, by 'custom, treaty, or other agreement'.[115] The US-UK Agreement appears to fall precisely within this scenario.[116] In *Big Brother Watch*, the ECtHR implied that this scenario may extend jurisdiction over the original impugned interference, which here might be, for example, the location at which a US service provider originally obtained data pursuant to a CLOUD Act regime request.[117] However, this has the same problem: the TCN is not in the US—where the service provider is—but is in a separate third jurisdiction.[118]

---

[111] Milanovic, 'Human Rights Treaties' (n 61) 126–127.

[112] ibid 124. See also Huxtable (n 100) 99.

[113] See Milanovic, 'Human Rights Treaties' (n 61) 124–125; Huxtable (n 100) 98–99.

[114] Milanovic, 'Human Rights Treaties' (n 61) 124–125.

[115] *Al-Skeini* (n 9) [135]. See also *Al-Sadoon* (n 8) [46]–[57].

[116] See Huxtable (n 100) 100.

[117] *Big Brother Watch* (n 36) [419]–[421].

[118] Watt (n 91) 102.

While Professor Marko Milanovic courageously argues that these models could be recalculated to apply in the digital sphere he acknowledges that it is by no means clear courts would follow his advice.[119] This ambiguity is precisely what enables the narrow approach to jurisdiction adopted in *Human Rights Watch*. The effect of this, supported by other UK cases,[120] is that TCNs are barred from bringing Article 8 claims before UK courts unless the interference with their digital privacy rights occurs when those TCNs are physically within UK territory.[121]

3.4.3 Recognition of a 'virtual jurisdiction' under Article 8 for TCNs here is justified

A reconceptualization of the ECHR's jurisdiction under Article 1 is required to ensure adequate protection of TCNs impacted by CLOUD Act regime requests. While it is beyond the scope of this thesis to detail a new Article 1 model,[122] any such model should include TCNs within the UK's new 'virtual jurisdiction' of Article 8 when acting under the CLOUD Act regime.

As Chapter 2 shows, there is a demonstrable protection gap for TCNs, which exists only because of their (assumed) physical location outside both US and UK territory. Under the CLOUD Act regime, however, the physical location of a target is immaterial and, indeed, will often be unknown.[123] Allowing UK persons but not TCNs to bring Article 8 claims creates an illogical protection gap. This is objectionable as a matter of principle. It is also inconsistent with the ECtHR's own jurisprudence, which recognises that Article 1

[119] Milanovic, 'Human Rights Treaties' (n 61) 121–130.

[120] *Zagorski* (n 13) [57]; *Sandiford* (n 13) [21]–[34]; *Akarcay* (n 13) [35]–[36].

[121] See Milanovic, 'UK Investigatory Powers Tribunal' (n 109); Raible, '*Human Rights Watch*' (n 12) 518.

[122] See generally eg Marko Milanovic, *Extraterritorial Application of Human Rights Treaties: Laws, Principles, and Policy* (OUP 2011); Besson (n 91); Lea Raible, *Human Rights Unbound: A Theory of Extraterritoriality* (OUP 2020).

[123] See n 33.

should not be interpreted allow for such gaps.[124] Yet the consequence of *Human Rights Watch* is to remove all manner of surveillance beyond the scope of the ECHR so long as it targets persons not physically within UK territory.[125] Even a UK person would lack Article 8 claims against its own state when they stepped outside UK territory.[126] These consequences strongly support reconceptualizing jurisdiction.

There are also affirmative reasons to reconceptualise ECHR jurisdiction in a way that recognises our increasingly digital world. The current approach to Article 1 is overly focused on *physical territory*,[127] yet data flows freely on cables and satellites across such multiple borders daily; it is 'de-territorialized'.[128] As Raible remarks, '[d]igital communications do not respect national borders and neither does government surveillance of such communications'.[129] The ECtHR has repeatedly emphasised the importance of providing practical supervision over rights, including Article 8, to respond to new technologies.[130] Technological developments 'have largely rendered the exercise of physical control over a location or an individual unnecessary'; significant interferences with digital privacy rights take place entirely 'virtually'.[131] This is true here. A CLOUD Act regime request enables the UK to directly target, or otherwise incidentally collect, sensitive personal data of people around the world. This in itself may implicate a TCN's digital privacy rights, and further breaches may follow should they be implicated in UK

[124] *Issa v Turkey* (2005) 41 EHHR 27 [71]. See also Aukje AH van Hoek & Michiel JJP Luchtman, 'Transnational cooperation in criminal matters and the safeguarding of human rights' (2005) 1(2) Utrecht L Rev 1, 18; Altwicker (n 109) 587; Wilson (n 100) 144; *Al-Sadoon* (n 8) [32] (following *Issa*).

[125] Wilson (n 100) 144.

[126] Milanovic, 'Human Rights Treaties' (n 61) 125.

[127] See Wilson (n 100) 144

[128] Ryngaert and van Eijk (n 105) 66.

[129] Raible, '*Human Rights Watch*' (n 12) 511. See also Humble (n 100) 10.

[130] See eg *Szabo and Vissy v Hungary* (2016) 63 EHRR 3 [62], [73], and [89]; *Zakharov v Russia* (2016) 63 EHRR 17 (GC) [229].

[131] McDermott (n 114) 202. See also Raible, '*Human Rights Watch*' (n 12) 518; Watt (n 91) 105.

criminal investigations.[132] Such persons deserve effective oversight and a real remedy by being brought within the ECHR's jurisdiction.[133] The ECtHR's existing extraterritorial models are impossible to justify in this era.[134]

3.5 Conclusion

This Chapter has argued for reconceptualising the Fourth Amendment and Article 8 to fill protection gaps for TCNs under the CLOUD Act regime. These gaps are significant and deprive TCNs of meaningful remedies should the US and UK unjustifiably interfere with TCNs' digital privacy rights. This situation should not be ignored by the US and UK. It is in their interests to respond to promote the long-term viability of the regime. In contrast, a failure to act now risks not only undermining the CLOUD Act regime but incentivising 'balkanisation' and similar developments. Overall, the approaches suggested above would be proportionate and justifiable in the context of both US and ECtHR jurisprudence. While these have been made in the particular context of the CLOUD Act regime, they indicate the importance of a broader need to reconceptualise extraterritoriality of rights mechanisms to properly enable digital privacy rights. Ultimately, it may not be too bold to suggest that, where our data flows, rights should follow.

[132] See *Big Brother Watch* (n 36) [419]–[421].

[133] See eg *Szabo* (n 130) [77].

[134] Raible, '*Human Rights Watch*' (n 12) 511.

BIBLIOGRAPHY

Books

Boister N, *An Introduction to Transnational Criminal Law* (2nd edn, OUP 2018)

Dickson B, *Human Rights and the United Kingdom Supreme Court* (OUP 2013)

Giannoulopoulos D, *Improperly Obtained Evidence in Anglo-American and Continental Law* (Hart Publishing 2019)

Krotoszynski Jr RJ, *Privacy Revisited: A Global Perspective on the Right to be Left Alone* (OUP 2016)

Milanovic M, *Extraterritorial Application of Human Rights Treaties: Laws, Principles, and Policy* (OUP 2011)

Nicholls C and others, *Nicholls, Montgomery, and Knowles on The Law of Extradition and Mutual Assistance* (3rd edn, OUP 2013)

Raible L, *Human Rights Unbound: A Theory of Extraterritoriality* (OUP 2020)

Scott PF, *The National Security Constitution* (Hart Publishing 2018)

Sottiaux S, *Terrorism and the Limitation of Rights: The ECHR and the US Constitution* (Hart Publishing 2008)

Trechsel S, *Human Rights in Criminal Proceedings* (OUP 2006)

Walden I, *Computer Crimes and Digital Investigations* (2nd edn, OUP 2016)

Zander M, *Zander on PACE: The Police and Criminal Evidence Act 1984* (8th edn, Sweet & Maxwell, 2018)

Zeegers K, *International Criminal Tribunals and Human Rights Law: Adherence and Tension* (Sprinter 2016)

Looseleaf services

Restatement of the Law – The Foreign Relations Law of the United States (draft 4th edn, 2020)

Search and Seizure: A Treatise on the Fourth Amendment (October 2019)

Book extracts

Bignami F and Resta G, 'Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance' in Eyel Benvenisti & Georg Nolte (eds) *Community Interests Across International Law* (OUP 2018)

Brunner L, 'Digital Communications and the Evolving Right to Privacy' in Molly K Land and Jay D Aronson (eds), *Digital Communications and the Evolving Right to Privacy* (CUP 2018)

Currie RJ, 'The protection of human rights in the suppression of transnational crime' in Neil Boister and Robert J Currie (eds), *Routledge handbook of transnational criminal law* (Routledge, Taylor and Francis Group 2015)

Daskal J, 'Transnational seizures: the constitution and criminal procedure abroad' in Federico Fabbrini and Vicki C Jackson (eds), *Constitutionalism across borders in the struggle against terrorism* (Elgar 2016) 192

——'*Microsoft Ireland* and content regulation: data territoriality and the best way forward' in Horatia Muir Watt and others (eds), *Global Private International Law: Adjudication Without Frontiers* (Edward Elgar 2019)

——and Vladeck SI, '"Incidental" Foreign Intelligence Surveillance and the Fourth Amendment' in David Gray and Stephen E Henderson (eds), *The Cambridge Handbook of Surveillance Law* (CUP 2017)

Dickson B, 'The extra-territorial obligations of European states regarding human rights in the context of terrorism' in Federico Fabbrini and Vicki Jackson (eds) *Constitutionalism Across Borders in the Struggle Against Terrorism* (Edward Elgar 2016)

Ferioli ML, 'Safeguarding defendants' rights in transnational and international cooperation' in Harmen van der Wilt and Christophe Paulussen (eds), *Legal Responses to Transnational and International Crimes: Towards an Integrative Approach* (Edward Elgar 2017)

Funk TM, 'The Key Tools of the Trade in Transnational Bribery Investigations and Prosecutions: Mutual Legal Assistance Treaties (MLATs) and Letters Rogatory' in T Markus Funk and Andrew S Boutros (eds), *Understanding the Global Fight Against Corruption and Graft* (OUP 2019)

Gless S and Macula L, 'Exclusionary Rules – Is it Time for Change? In Sabine Gless and Thomas Richter (eds), *Do Exclusionary Rules Ensure a Fair Trial?: A Comparative Perspective on Evidentiary Rules* (Springer 2019)

Hafetz J, 'The Possibilities and Limits of Corporations as Privacy Protectors in the Digital Age' in David Cole, Feredico Fabbrini and Stephen Schulhofer (eds), *Surveillance, Privacy and Trans-Atlantic Relations* (Hart Publishing 2019)

Hughes K, 'A Common Law Constitutional Right to Privacy – Waiting for Godot?' in Mark Elliott and Kirsty Hughes (eds) *Common Law Constitutional Rights* (Hart Publishing 2020)

Jackson VJ, 'Translating rights across centuries: U.S. constitutional protection against unreasonable searches and seizures in a transnational era' in Federico Fabbrini and Vicki C Jackson (eds), *Constitutionalism across borders in the struggle against terrorism* (Elgar 2016)

Lynsky O, ‘Courts, privacy and data protection in the UK’ in Maja Brkan and Evangelia Pscyhogiopodou (eds), *Courts, Privacy and Data Protection in the Digital Environment* (Edward Elgar 2017)

McCullagh K, ‘Post-Brexit Data Protection in the UK’ in Gloria Gonzalez Fuster and others (eds), *Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics* (Edward Elgar, forthcoming)

McDermott H, ‘Application of the International Human Rights Law Framework in Cyber Space’ in Dapo Akande and others (eds), *Human Rights and 21st Century Challenges* (OUP 2020)

Milanovic M, ‘Jurisdiction and Responsibility: Trends in the Jurisprudence of the Strasbourg Court’, in Anne van Aaken and Iulia Motoc (eds), *The European Convention on Human Rights and General International Law* (OUP 2018) 102

Psychogiopoulou E, ‘The European Court of Human Rights, privacy and data protection in the digital era’ in Maja Brkan and Evangelia Pscyhogiopodou (eds), *Courts, Privacy and Data Protection in the Digital Environment* (Edward Elgar 2017)

Stephen A, ‘Enforcing Criminal Jurisdiction in the Clouds and International Law’s Enduring Commitment to Territoriality’ in Stephen Allen and others (eds), *The Oxford Handbook of Jurisdiction in International Law* (OUP 2019)

Turner JI, ‘Regulating Interrogations and Excluding Confessions in the United States: Balancing Individual Rights and the Search for the Truth’ in Sabine Gless and Thomas Richter (eds), *Do Exclusionary Rules Ensure a Fair Trial?: A Comparative Perspective on Evidentiary Rules* (Springer 2019)

Vervaele JAE, ‘Mutual legal assistance in criminal matters to control (transnational) criminality)’ in Neil Boister and Robert Currie (eds), *Routledge Handbook of Transnational Criminal Law* (Routledge 2014)

Watt E, ‘The Role of International Human Rights Law in the Protection of Online Privacy in the Age of Surveillance’ in H. Rõigas and others (eds), *2017 9th International Conference on Cyber Conflict: Defending the Core* (NATO CCD COE 2017)

Woods AK, ‘Mutual Legal Assistance in the Digital Age’ in David Gray and Stephen E Henderson (eds), *The Cambridge Handbook of Surveillance Law* (CUP 2017)

Journal Articles

Abraha HH, ‘Regulating law enforcement access to electronic evidence across borders: the United States approach’ (2020) Info & Coms Tech L (forthcoming)

Akehurst M, ‘Jurisdiction in International Law’ (1972-1973) British Yearbook of Int L 145

Altwicker T, ‘Transnationalizing Rights: International Human Rights Law in Cross-Border Contexts’ (2018) 29 EJIL 581

Bellia PL, ‘Chasing Bits Across Borders’ (2001) U Chi Legal F 35

Besson S, ‘The Extraterritoriality of the European Convention on Human Rights: Why Human Rights Depend on Jurisdiction and What Jurisdiction Amounts to’ (2012) 25 Leiden J of Intl L 857

Bignami F and Resta G, ‘Transatlantic Privacy Regulation: Conflict and Cooperation’ (2015) 78 L Contemporary Problems 21

Bilgic S, ‘Something Old, Something New, and Something Moot: The Privacy Crisis Under the CLOUD Act’ (2018) 32 Harv J of L & Tech 321

Bomhoff J, ‘The Reach of Rights: “The Foreign” and “The Private” in Conflict-of-Laws, State-Action, and Fundamental-Rights Cases With Foreign Elements’ (2008) 71 L & Cont Probs 39

Connor IR, ‘Peoples Divided: The Application of United States Constitutional Protections in International Criminal Law Enforcement’ (2002) 11 Wm & Mary Bill of Rts J 495

Currie RJ, Currie RJ, ‘Human Rights and International Legal Assistance: Resolving the Tension’ (2000) 11 Crim L Forum 143

——‘Charter Without Borders? The Supreme Court of Canada, Transnational Crime and Constitutional Rights and Freedoms’ (2004) 27 Dal LJ 235

——‘Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the Next Frontier’ (2016) 54 Can YB Intl L 63

Daskal J, ‘The Un-Territoriality of Data’ (2015) 125 Yale L J 326

——‘Law Enforcement Access to Data Across Borders: the Evolving Security and Rights Issues’ (2016) 8 J of Nat Sec L & Poly 473

——‘Notice and Standing in the Fourth Amendment: Searches of Personal Data’ (2017) 26 Wm & Mary Bill Rts J 437

——‘Borders and Bits’ (2018) 71 Vanderbilt L Rev 179

——‘*Microsoft Ireland*, CLOUD Act, and International Law-Making 2.0’ (2018) 71 Stan L Rev Online 9

——‘Privacy and Security Across Borders’ (1 April 2019) 128 Yale L J Forum 1029

——‘Transnational Government Hacking’ (2020) 10 J Nat Sec L & Poly 677

David C, ‘Are Foreigners Entitled to the Same Constitutional Rights As Citizens?’ (2003) 25 T Jefferson L Rev 367

Davidson A, ‘Extraterritoriality and statutory interpretation: the increasing reach of investigative powers’ [2020] PL 1.

Davis FT and Gressel AR, ‘Storm Clouds or Silver Linings? The Impact of the U.S. Cloud Act’ [Fall 2018] Litigation 47

de Busser E, ‘The Digital Unfitness of Mutual Legal Assistance’ (2017) 28 Sec and Human Rts 161

——‘EU-US Digital Data Exchange to Combat Financial Crime: Fast is the New Slow’ (2018) 19 German LJ 1251

Donohue LK, ‘The Fourth Amendment in a Digital World’ (2017) 71 NYU Ann Survy Am L 553

Galvagna C, ‘The Necessity of Human Rights Legal Protections in Mutual Legal Assistance Reform’ (2019) 9 Notre Dame J of Intl & Comp L 57

Gane C and Mackarel M, ‘The Admissibility of Evidence Obtained from Abroad into Criminal Proceedings – The Interpretation of Mutual Legal Assistance Treaties and Use of Evidence Irregularly Obtained’ (1994) 4 Eur J Crime, Crim L & Crim Just 98

Halpen AS, ‘Secret Searches: The SCA’s Standing Conundrum’ (2010) 17 Mich L Rev 1696

Hemmings J, Srinivasan S and Swire P, ‘Defining the Scope of “Possession, Custody, or Control” for Privacy Issues and the CLOUD Act’ (2020) 10 J of Natl Sec L and Poly 631

Holmes AM, ‘Private actor or public authority? How the status of communications service providers affects human rights’ (2017) 22 Comms L 21

Humble KP, ‘International law, surveillance and the protection of privacy’ (2020) Int J of Hum Rts (forthcoming)

Huxtable H, ‘E.T. Phone Home…They Know: The Extraterritorial Application of Human Rights Treaties in the Context of Foreign Surveillance’ (2017) 28 Sec and Hum Rts 92

Kerr OS, ‘Lifting the “Fog” of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law’ (2003) 54 Hastings LJ 805

——‘A User’s Guide to the Stored Communications Act, and A Legislator’s Guide to Amending It’ (2004) 72 Geo Wash L Rev 1208

——‘The Fourth Amendment and the Global Internet’ (2015) 67 Stan L Rev 285

Kim EB, ‘U.S.-U.K. Executive Agreement: Case Study of Incidental Collection of Data Under the CLOUD Act’ (2020) 15 Wash J of L, Tech & Arts 247

Kopel M, ‘Injustice at the Border: Application of the Constitution Abroad through the Conflict of Laws’ (2019) 167 U Pa L Rev 1241

Marouf FE, ‘Extraterritorial Rights in Border Enforcement’ (2020) 77 Wash & Lee L Rev 751

Milanovic M, ‘Al-Skeini and Al-Jedda in Strasbourg’ (2012) 23 EJIL 121

——‘Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age’ 56 (2015) Harv Intl L J 81

Mills A, ‘Crime (Overseas Production Orders) Act 2039: The Increasing Relevance of UK Investigatory Powers to those Advising Businesses and Individuals’ (2019) 9 JIBFL 624, 624.

O’Leary S, ‘Balancing rights in the digital age’ (2018) Irish Jurist 59

Pope AE, ‘Lawlessness Breeds Lawlessness: A Case for Applying the Fourth Amendment to Extraterritorial Searches’ (2013) 65 Fla L Rev 1917

Prabhu JV, Berrang AP, and Dickey R, ‘When Your Cyber Case Goes Abroad: Solutions to Common Problems in Foreign Investigations’ (2019) 67 DOJ J Fed L and Prac 167

Raible L, ‘The Extraterritoriality of the ECHR: Why Jaloud and Pisari should be Read as Game Changers’ [2016] Eur Hum Rts L Rev 161

——‘*Human Rights Watch v Secretary of State for the Foreign and Commonwealth Office*: Victim Status, Extraterritoriality and the Search for Principled Reasoning’ (2017) 80 MLR 510

Ramcharan, Bertrand G, ‘The Universality of Human Rights’ (1994) 53 The Review 105

Ronchi P, ‘The Borders of Human Rights’ (2012) 128 LQR 20

Ryngaert CMJ, and van Eijk NANM, ‘International cooperation by (European) security and intelligence services: reviewing the creation of a joint database in light of data protection guarantees’ (2019) 9 Intl Data Privacy L 61

Schaefer M, ‘Al-Skeini and the elusive parameters of extraterritorial jurisdiction’ (2011) 5 EHRLR 556

Schwartz PM, ‘Legal Access to the Global Cloud’ (2018) 118 Colum L Rev 1681

——‘Global Data Privacy: The EU Way’ (2019) 94 NY L Rev 771

Siry L, ‘Cloudy days ahead: Cross-border evidence collection and its impact on the rights of EU citizens’ (2019) 10 NJECL 227

Smith A, ‘Overseas Production Orders: getting up to speed’ (2019) 169 NLJ 8730

Snow TG, ‘The Investigation and Prosecution of White Collar Crime: International Challenges and the Legal Tools Available to Address Them’ (2002) 11 Wm & Marty Bill Rts J 207

Stanislaw T, ‘Mutual recognition by private actors in criminal justice? Service providers as gatekeepers of data and human rights obligations’ (2020) CML Rev (forthcoming).

Swire P and Hemmings J, ‘Mutual Legal Assistance In an Era of Globalized Communications: The Analogy To the Visa Waiver Program (2017) 71 NYU Ann Surv of American L 687

Swire P and Kennedy-Mayo D, ‘How Both the EU and the U.S. Are Stricter than Each Other for the Privacy of Government Requests for Information’ (2017) 66 Emory LJ 617

van Hoek AAH, & Luchtman MJJP, ‘Transnational cooperation in criminal matters and the safeguarding of human rights’ (2005) 1(2) Utrecht L Rev 1

Warren S, and Brandeis L, ‘The Right to Privacy’ (1890) 4 Harv L Rev 193

Wilson K, ‘The European Convention on Human Rights and the Investigatory Powers Tribunal: Rationalising a Law unto Itself?’ (2020) 23 Trinity CL Rev 129

Woods AK, ‘Litigating Data Sovereignty’ (2018) 28 Yale L J 328

Zagaris B ‘U.S. Government's Ability to Obtain and Provide International Enforcement Constrained By Budget, Failure to Meet International Standards, and Join International Initiatives’ (2015) 31 Intl Enforcement L Reporter 514

Blog Posts

Christakis T, ’21 Thoughts and Questions about the UK-US CLOUD Act Agreement (and an Explanation of how it Works – with Charts)’ (*European Law Blog*, 17 October 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/> accessed 31 July 2020

——‘E-EVIDENCE: THE WAY FORWARD (Summary of the Workshop Held in Brussels on 25 September 2019) (*European Law Blog*, 6 November 2019) <https://europeanlawblog.eu/2019/11/06/e-evidence-the-way-forward-summary-of-the-workshop-held-in-brussels-on-25-september-2019/> accessed 31 July 2020

——and Propp K, ‘The Legal Nature of the UK-US CLOUD Agreement’ (*Cross-Border Data Forum*, 20 April 2020) <www.crossborderdataforum.org/the-legal-nature-of-the-uk-us-cloud-agreement> accessed 31 July 2020

Daskal J, ‘Correcting the Record: Wiretaps, the CLOUD Act, and the US-UK Agreement’ (*JustSecurity*, 31 October 2019) <www.justsecurity.org/66774/correcting-the-record-wiretaps-the-cloud-act-and-the-us-uk-agreement/> accessed 31 July 2020

——and Woods AK, ‘Cross-Border Data Requests: A Proposed Framework’ (*LawFare*, 24 November 2015) <www.lawfareblog.com/cross-border-data-requests-proposed-framework> accessed 31 July 2020

——and Woods AK, ‘Congress Should Embrace the DOJ’s Cross-Border Data Fix’ (*LawFare*, 1 August 2016) <www.lawfareblog.com/congress-should-embrace-dojs-cross-border-data-fix-0> accessed 31 July 2020

——and Swire P, ‘Privacy and Civil Liberties Under the CLOUD Act: A Response’ (LawFare, 21 March 2018) <www.lawfareblog.com/privacy-and-civil-liberties-under-cloud-act-response> accessed 31 July 2020

——and Swire P, ‘The U.K.-U.S. CLOUD Act Agreement Is Finally Here, Containing New Safeguards’ (*LawFare*, 8 October 2019) <www.lawfareblog.com/uk-us-cloud-act-agreement-finally-here-containing-new-safeguards> accessed 31 July 2020

Gidari A, ‘The Big Interception Flaw in the US-UK CLOUD Act Agreement’ (*The Center for Internet and Society*, 18 October 2019) <http://cyberlaw.stanford.edu/blog/2019/10/big-interception-flaw-us-uk-cloud-act-agreement> accessed 31 July 2020

——‘More Questions About the CLOUD Act and the US-UK Agreement – Can the US Direct UK Providers to Wiretap Their Users in Third Countries?’ (*The Center for Internet and Society*, 13 November 2019) <http://cyberlaw.stanford.edu/blog/2019/11/more-

questions-about-cloud-act-and-us-uk-agreement-can-us-direct-uk-providers-wiretap> accessed 31 July 2020

——'Can the US-UK CLOUD Act Agreement Be Fixed?' (*The Center for Internet and Society*, 18 November 2019) <http://cyberlaw.stanford.edu/blog/2019/11/can-us-uk-cloud-act-agreement-be-fixed> accessed 31 July 2020

Farrell H and Newman AL, 'Schrems II Offers an Opportunity – If the U.S. Wants to Take It' (*LawFare*, 28 July 2020) < www.lawfareblog.com/schrems-ii-offers-opportunity-if-us-wants-take-it> accessed 31 July 2020.

Greaves P and Swire P, 'New Developments for the U.K. and Australian Executive Agreements with the U.S. Under the CLOUD Act' (*Cross-Border Data Forum*, 19 July 2020) <www.crossborderdataforum.org/new-developments-for-the-u-k-and-australian-executive-agreements-with-the-u-s-under-the-cloud-act-2/> accessed 31 July 2020

Kent G, 'The Mutual Legal Assistance Problem Explained' (*The Center for Internet and Society*, 23 February 2015) <http://cyberlaw.stanford.edu/blog/2015/02/mutual-legal-assistance-problem-explained> accessed 31 July 2020

Milanovic M, 'UK Investigatory Powers Tribunal Rules that Non-UK Residents Have No Right to Privacy under the ECHR' (*EJIL:Talk!*, 18 May 2016) <www.ejiltalk.org/uk-investigatory-powers-tribunal-rules-that-non-uk-residents-have-no-right-to-privacy-under-the-echr/> accessed 31 July 2020

Niblock R, 'On its way: The UK-US Bilateral Data Access Agreement' (*Kingsley Napley Criminal Law Blog*, 31 July 2020)

Smith B 'A call for principle-based international agreements to govern law enforcement access to data (*Microsoft On the Issues*, 11 September 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/> accessed 31 July 2020

Swindon S, 'Police can access suspects' Facebook and WhatsApp messages in deal with US' (The Times, 28 September 2019) <www.thetimes.co.uk/edition/news/police-can-access-suspects-facebook-and-whatsapp-messages-in-deal-with-us> accessed 31 July 2020

Tyler AL, 'Thuraissigiam and the Future of the Suspension Clause' (LawFare, 2 July 2020) <www.lawfareblog.com/thuraissigiam-and-future-suspension-clause> accessed 31 July 2020

Westmoreland K, 'Are Some Companies "Yes Men" When Foreign Governments Ask for User Data?' (*The Center for Internet and Society*, 30 May 2014) <http://cyberlaw.stanford.edu/blog/2014/05/are-some-companies-yes-men-when-foreign-governments-ask-user-data> accessed 31 July 2020

Woods AK, and Swire P, 'The CLOUD Act: A Welcome Legislative Fix for Cross-Border Data Problems' (LawFare, 6 February 2018) <www.lawfareblog.com/cloud-act-welcome-legislative-fix-cross-border-data-problems> accessed 31 July 2020

Reports

Anderson D, *A Question of Trust: Report of the Investigatory Powers Review* (June 2015)

Clarke RA and others, *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies* (12 December 2013)

Report of the Office of the United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, UN Doc A/HRC/27/37 (30 June 2014)

Stefan M and Fuster GG, 'Cross-border Access to Electronic Data through Judicial Cooperation in Criminal Matters' (CEPS Paper No 2018-07, November 2018, updated May 2019)

Swire P and Hemmings J, 'Overcoming Constitutional Objections to the CLOUD Act' (American Constitution Society, Issue Brief, February 2020)

Swire P, Woo J and Desai DR, 'The Important, Justifiable, and Constrained Role of Nationality in Foreign Intelligence Surveillance (Aegis Series Paper No 1901, Hoover Institution, 2019)

Parliamentary and congressional records and related publications

163 Cong Rec S7939 (daily ed 1 December 2017)

164 Cong Rec S1923 (daily ed 22 March 2018)

164 Cong Rec. S595 (daily ed 5 February 2018)

HL Deb 11 July 2018, vol 792, col 927

HL Deb 20 November 2018, vol 794, cols 140 and 142

HC Deb 18 December 2018, vol 651, col 13

HC Deb 30 January 2019 vol 653, cols 852 and 859–860

US House of Representatives, 'Email Privacy Act' (HOR 114th Congress, 2d Sess, 114–528)

Mulligan SP, Cross-Border Data Sharing Under the CLOUD Act (Congressional Research Service, 7–500 23 April 2018)

Newsom N, 'Crime (Overseas Production Orders) Bill' (*House of Lords Library Briefing*, 5 July 2018)

European Commission, 'Answer to Parliamentary questions given by Mr Reynders' (E-003136/2019, 10 January 2020)]

Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (Australia)

Government publications

Cabinet Office, *Summary of the Work of the Prime Minister's Special Enjoy on Intelligence and Law Enforcement Data Sharing – Sir Nigel Sheinwald* (25 June 2015)

Crown Prosecution Service, 'International Enquiries' *The Code for Crown Prosecutors* (1 July 2019) <www.cps.gov.uk/legal-guidance/international-enquiries>

US Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (Version 3, 2009)

——'Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act' (White Paper, April 2019)

——'Joint US-EU Statement on Electronic Evidence Sharing Negotiations' (26 September 2019)

——'U.S. and UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online' (3 October 2019) <www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists> accessed 31 July 2020

——'Joint Statement Announcing United States and Australian Negotiation of a CLOUD Act Agreement by U.S. Attorney General William Barr and Minister for Home Affairs Peter Dutton' (7 October 2019)

——*Justice Manual* (last updated January 2020)

Foreign and 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)

UK Home Office, *Requests for Mutual Legal Assistance in Criminal Matters: Guidelines for Authorities Outside of the United Kingdom* (12th edn, March 2015)

——*Crime (Overseas Production Orders) Bill 2018: Overarching Fact Sheet* (September 2018)

——*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)

Correspondence

Letter from Apple and others to Senator Orrin Hatch and others (6 February 2018) <https://tinyurl.com/y5k63rvk> accessed 31 July 2020

Letter from Peter J Kadzik, US Assistant Attorney Gen, to the Hon Joseph R Biden, President, US Senate (July 15, 2016) <https://tinyurl.com/y7b7fhaw> accessed 31 July 2020

Letter from Samuel R Ramer, Acting Assistant Attorney General, to Hon Paul Ryan, Speaker, US House of Representatives (24 May 2017) <https://perma.cc/MUT6-A8GC> accessed 31 July 2020

Letter to Richard W Downing, Acting Deputy Assistant Attorney General, from Human Rights Watch and others (28 November 2018) <https://tinyurl.com/yygyprtd> accessed 31 July 2020

Speeches and Presentations

Daskal J and others, 'Panel 5: Extraterritorial Application of U.S. Law to the Cloud' (*Symposium on Government Access to Data in the Cloud*, NYU School of Law, 29 May 2015) <www.youtube.com/watch?v=0U5WOYNQCaQ> accessed 31 July 2020

Downing R, Assistant Attorney General, 'Prospects for Transatlantic Cooperation on the Transfer of Electronic Evidence to Promote Public Safety' (Academy of European Law Conference, London, UK, 5 April 2019).

——and others, Remarks at panel discussion on 'Globalization of Criminal Evidence' (Privacy + Security Academy, Washington DC, 15 October 2019)

McGuinness P, UK Deputy National Security Adviser, 'Written Testimony' (Judicial Sub-Committee on Crime and terrorism, US Senate, 10 May 2017)

Miscellaneous

ECtHR, 'Grand Chamber hearing on complaints about surveillance systems in the case of Big Brother Watch and Others v. the United Kingdom' (ECHR 258 (2019), 10 July 2019)

US' Trial Brief *US v Nikulin* 2020 WL 1910377, No CR 16 – 00440 WHA (ND Cal, 3 March 2020)

Dropbox, 'Transparency at Dropbox – Reports' (2019) <www.dropbox.com/transparency/reports> accessed 31 July 2020