The final version of this paper has been published in the New Zealand Law Review as: Tim Cochrane, 'Law Enforcement Cross-Border Data Sharing: A CLOUD Act Agreement for Aotearoa New Zealand?' [2021] NZLR 401. Please cite only to that published version.

Law Enforcement Cross-Border Data Sharing: A CLOUD Act Agreement for New Zealand?

Tim Cochrane*

This article considers whether New Zealand should seek a 'CLOUD Act' agreement with the United States. These agreements aim to speed up law enforcement access to overseas electronic data while protecting privacy and enhancing civil liberties. CLOUD Act agreements, like other new 'direct access' mechanisms being proposed internationally, respond to concerns with the "slow and cumbersome" nature of the main existing tool law enforcement have to access such data, mutual legal assistance (MLA). This article begins by discussing key background contexts. It then outlines the CLOUD Act regime, considering how New Zealand could implement a hypothetical US-NZ CLOUD Act Agreement. It finally evaluates potential advantages and risks for New Zealand. Overall, while a US-NZ Agreement would provide benefits, it may significantly undermine the digital privacy rights of New Zealanders and others relative to MLA. New Zealand should exercise caution.

I Introduction

This article considers whether New Zealand should seek a 'CLOUD Act' agreement with the United States. This new international law enforcement data sharing regime—named after its enabling United States legislation, the Clarifying Lawful Overseas Use of Data Act 2018 (**CLOUD Act**)—responds to difficulties law enforcement face in obtaining overseas electronic data. The main existing method, mutual legal assistance (**MLA**),[1] can take months or even years. The CLOUD Act regime aims to "reduce this time period considerably, while protecting privacy and enhancing civil liberties", through bilateral agreements allowing one state's law enforcement to directly enforce their own orders for the preservation, disclosure, or interception of electronic data against overseas service providers operating in the other state.[2]

This is not a mere trans-Atlantic phenomenon. While only one bilateral agreement currently exists, between the United States and United Kingdom (**US-UK Agreement**),[3] they hope to expand the regime to other "rights-respecting countries", including New Zealand.[4] The

* PhD Law Candidate (Cantab); MPhil Law (Dist) (Oxon); LLM (Dist) (UPenn); LLB/BA(Hons) (Otago); Attorney & Counselor-at-Law, New York State; Solicitor, Senior Courts of England and Wales; and Barrister and Solicitor of the High Court of New Zealand. This article was made possible through the generous funding provided by the Office of the Privacy Commissioner's Privacy Good Research Fund 2019. A draft was presented at the Victoria University of Wellington Faculty of Law on 23 August 2020, available online at <www.youtube.com>. This article has benefited from feedback provided from attendees and others following that presentation. The author would also like to thank Amelia Retter and Jean Thompson of Dentons Kensington Swan for research assistance.

[1] See generally Neil Boister *Introduction to Transnational Criminal Law* (2nd ed, Oxford University Press, Oxford, 2018) at chs 17 and 18; and New Zealand Government *What is Mutual Assistance?* (15 July 2020).

[2] United States Department of Justice [**USDOJ**] "U.S. and UK Sign Landmark Cross Border Data Access Agreement to Combat Criminals and Terrorists Online" (3 October 2019) <www.justice.gov>.

[3] United Kingdom Foreign and Commonwealth Office [**UKFCO**] *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**].

[4] USDOJ *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act* (White Paper, April 2019) [***US White Paper***] at 11; and United Kingdom Home Office *Impact*

Ministry of Justice and Law Commission have suggested CLOUD Act agreements may be "the appropriate mechanism for dealing with many of the issues" law enforcement face in obtaining overseas data.[5] Australia is already negotiating a bilateral agreement with the United States.[6] The regime's 'direct access' nature is also mirrored in other international proposals, including a draft Second Additional Protocol to the Budapest Convention on Cybercrime (**Budapest Convention**), which New Zealand will shortly join.[7]

This article focuses on how a CLOUD Act agreement between the United States and New Zealand (**US-NZ Agreement**) may impact digital privacy rights—meaning the developing rights of privacy over electronic data and the devices on which they are contained. It is uncontroversial that New Zealand should take into account privacy and other rights when drafting policy, legislation, and treaties[8]—all areas engaged here. This article also builds on existing research evaluating the impact of this regime for similar rights under United States and United Kingdom law.[9] Part II provides background, outlining why and how law enforcement seek overseas data and how digital privacy is impacted they do. Part III explains the CLOUD Act regime, discussing its background, operation, and rights protections, and then imagines how a hypothetical US-NZ Agreement could be implemented in New Zealand. Finally, Part IV evaluates potential benefits and risks for New Zealand, recommending that New Zealand exercises caution, given the potentially significant negative impact a US-NZ Agreement may have on digital privacy.

II Electronic Data, MLA, and Digital Privacy

A *Electronic data and criminal investigations*

New Zealand criminal investigations commonly rely on electronic data,[10] a consequence of the ubiquitous use of electronic communications by criminals.[11] Data is crucial in securing

---

Assessment: Crime (Overseas Production Orders) Bill (HO315, 11 May 2018) at 5. See also (22 March 2018) 164 Cong. Rec. S1923 (daily ed); and (11 July 2018) 792 GBPD HL 921.

[5] Law Commission and Ministry of Justice [**MOJ**] *Review of the Search and Surveillance Act 2010 Ko Te Arotake I Te Search and Surveillance Act 2012* (NZLC R141, 2018) [**SSA Report**] at [14.159]. See also New Zealand Government *Why is New Zealand considering joining the Budapest Convention?* (15 July 2020) at 2–3.

[6] USDOJ "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" (press release, DOJ19-1075, 7 October 2019). See also Australian Commonwealth, *Parliamentary Debates*, House of Representatives, 5 March 2020, 2467–2469, Alan Tudge MP.

[7] See Cabinet Office Circular "Council of Europe Convention on Cybercrime: Approval to Accede" (22 January 2021) CBC-20-MIN-0129 at [27] and [36]. See generally Convention on Cybercrime 2296 UNTS 167 (opened for signature 23 November 2011, entered into force 1 July 2004).

[8] Cabinet Office *Cabinet Manual 2017* at [7.65]–[7,67], [7.123] and [7.133]. See generally New Zealand Bill of Rights Act 199 [**Bill of Rights**], ss 3, 5 and 6; Legislation Design and Advisory Committee [**LDAC**] *Legislation Guidelines 2018 Edition* (March 2018); Department of Prime Minister and Cabinet [**DPMC**] "Human Rights compliance in bills and Cabinet Papers" (*CabGuide*, 16 July 2019); and Ministry of Foreign Affairs and Trade [**MFAT**] *International Treaty Making: Guidance for government agencies on practice and procedures for concluding international treaties and arrangements* (September 2020).

[9] Tim Cochrane "Digital Privacy Rights and the CLOUD Act Regime" (2022) 47 Brooklyn J of Intl L (forthcoming) (manuscript on file with author).

[10] SSA Report, above n 5, at [2.64] and [14.49]. See *R v Marsh* HC Auckland CRI-2006-004-005881, 19 December 2007 at [24]; *R v Bogue* [2014] NZHC 826 at [5]; *Neho v R* [2017] NZCA 324 at [17]; *Fenwick v Police* [2017] NZHC 992 at [36]; *R v Siulai* [2018] NZDC 3728, [2019] DCR 555 at [49]; and *Parker v R* [2020] NZHC 1345 at [2].

[11] See *R v McFall* [2005] DCR 823 (HC) at [48]; *R v Javid* HC Auckland CRI-2005-004-019217, 3 March 2006 at [25]; *Hoete v R* [2013] NZCA 432, (2014) 26 CRNZ 429 at [20] and [32]; and *R v F* [2018] NZHC 2602 at

convictions in more cases each year.[12] Some, such as call, text, and polling data, are ordinarily transmitted through New Zealand service providers and can be readily obtained by law enforcement from these providers without 'tipping-off' suspects,[13] typically using 'production orders' under the Search and Surveillance Act 2012 (**SSA**).[14] These are similar to traditional search warrants, available where law enforcement satisfy a court (or other independent issuing officer) that various reasonable grounds justifying the order are made out.[15] However, unlike search warrants—normally executed by law enforcement directly—production orders are regularly executed indirectly by "co-operative" third parties, including service providers.[16] Law enforcement may also intercept data during transmission using SSA "surveillance device warrants".[17] Where data is transmitted through telecommunications providers—a subset of service providers[18]—the Telecommunications (Interception Capability and Security) Act 2013 (**TICSA**) imposes an express statutory duty on providers to assist with intercepts.[19]

Electronic data held by overseas service providers is increasingly important for criminal investigations.[20] The contents of electronic communications processed by such providers are often sought as evidence in prosecutions, including not only emails,[21] but communications transmitted through social media applications like WhatsApp,[22] Facebook,[23] Instagram,[24]

---

[15]–[16]. See also Ko tō tātou kāinga tēnei *Report of the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019* (26 November 2020) at 533.

[12] See *W (CA597/2016) v R* [2017] NZCA 118 at [25]. See for example *R v Namana* [2019] NZHC 1952.

[13] Privacy Commissioner *Releasing personal information to Police and law enforcement agencies: Guidance on health and safety and Maintenance of the law exceptions* (October 2017, updated December 2017) at 3; and *Tupoumalohi v R* [2020] NZCA 641 at [21]. See *R v Reti* [2020] NZSC 16 at [40]. But see also *Song v R* [2016] NZCA 631 at [28].

[14] Search and Surveillance Act 2012 [**SSA]**, ss 70–79; *R v Alsford* [2017] NZSC 42, [2017] 1 NZLR 710 at [18]–[20]; and Police Manual [**PM]** *Search Part 9 – Production Orders* (Obtained on 17 June 2020 under Official Information Act 1982 [**OIA]** Request to the Police) at 6. See also SSA Report, above n 5, at [14.11]. See generally *R v Catley* [2016] NZHC 2935] at [7]–[17].

[15] SSA, s 72; and *Reti*, above n 12, at [36]–[40]. See SSA, s 3 (defining "issuing officer"). See generally SSA Report, above n 5, at ch 14.

[16] SSA, s 75. See Law Commission, *Search and Surveillance Powers* (NZLC R97, June 2007) at [10.22]–[10.28]; and SSA Report, above n n 5, at [14.7] and [14.11].

[17] SSA, ss 45–64.

[18] Compare Telecommunications (Interception Capability and Security) Act 2013 [**TICSA**], s 3(1) (definitions of "telecommunication" and "service provider"), with US-UK Agreement, above n 3, at arts 1(3) and (5) (definitions of "Covered Data" and "Covered Provider").

[19] TICSA, s 24. See also ss 3(1) (definition of "interception warrant"); and Michael Dizon and others *A matter of security, privacy and trust: A study of the principles and values of encryption in New Zealand* (December 2019) at 73–75.

[20] Cabinet Office, above n 7, at [17]–[18]. See New Zealand Government, above n 5, at 2; and New Zealand Police *Briefing to the Incoming Minister of Police: Part B Key operational priorities* (November 2020) at B-7. See generally (16 October 2013) 694 NZPD 13967.

[21] See for example *R v Karpacavicius* [2013] NZHC 1996 at [15] and [19]–[20].

[22] See for example *R v Nguyen* [2018] NZDC 4632 at [12]; and *Parker*, above n 10, at [24].

[23] See for example *Holland v Police* [2017] NZHC 2284 at [6]; *Hogg v R* [2019] NZHC 1254 at [5] and [14]; *Namana*, above n 12, at [25]; and *Ngapuhi v Police* [2019] NZHC 2177 at [46].

[24] See for example *Vujcich v New Zealand Police* [2019] NZHC 2482 at [6]–[7].

Snapchat,[25] Facetime,[26] Viber,[27] and Wickr.[28] However, New Zealand law enforcement have limited options for obtaining such data. An electronic device containing the data may be seized and searched,[29] but this may alert suspects to an ongoing investigation.[30] Data may be deleted, or the device destroyed altogether, before the search occurs.[31] Other options include obtaining data by consent,[32] or using interception devices,[33] but these often have limited utility.[34]

It is New Zealand policy to use MLA when seeking data as evidence from overseas service providers.[35] It cannot simply compel overseas service providers using an SSA production order or similar process. Enforcing compulsory legal process against overseas persons is traditionally viewed as breaching the prohibition against unilateral extraterritorial "enforcement jurisdiction" at customary international law,[36] although the continued application of this prohibition to cross-border data requests is unclear.[37] Additionally, consistent with the presumption against extraterritorially,[38] production orders appear to not extend extraterritorially—ie outside New Zealand territory[39]—to reach foreign service providers.[40] While the Court of Appeal has made contrary comments,[41] these appear inconsistent with that presumption and have been criticised.[42] In any event, overseas providers, typically based in

[25] See for example *Namana*, above n 12, at [95] and [140].

[26] See for example *R v F*, above n 10, at [16].

[27] See for example *R v Tran* [2016] NZHC 680 at [35] n.9; and *Ngapuhi*, above n 23, at [28]–[32] and [45].

[28] See for example *R v F*, above n 10, at [16]; and *Parker*, above n 10, at [30].

[29] SSA, ss 6–32, 82–88, and 97–109. See for example *Ngapuhi*, above n 23, at [40]; *Hogg*, above n 23, at [38]; and *Parker*, above n 10, at [24]. See also *Leslie v R* [2018] NZCA 224 at [43]–[46]; and *Ruru v R* [2020] NZCA 64 at [88]–[97].

[30] See above n 12.

[31] See for example *Holland*, above n 23, at [6]; *Tran*, above n 27, at [38]; *Mehrtens v R* [2018] NZCA 446 at [6](c) and [20]; *New Zealand Police v Hepi* [2019] NZDC 1075 at [13]; and *Parker*, above n 10, at [21] and [30].

[32] See for example *Ngapuhi*, above n 23, at [31].

[33] SSA, ss 3(1) (definition of "interception device") and 46(1). See for example *Karpacavicius*, above n 21, at [8]; *Namana*, above n 12, at [25]; and *R v F*, above n 10, at [5]. See also SSA Report, above n 5, at [7.37]–[7.55].

[34] See for example *Namana*, above n 22, at [26] and [95].

[35] PM *Search Part 5*, above n 43, at 32. See Cabinet Office above n 14, at [18]; PM *INTERPOL* (Obtained on 17 June 2020 under OIA Request to the Police) at 24; and Letter from Greg Dalziel (Detective Senior Sergeant, High Tech Crime Group, Police National Headquarters) to author regarding OIA request (17 June 2020).

[36] Boister, above n 1, at 328–329; SSA Report, above n 5, at [12.76] and n. 76; and Alberto Costi "Jurisdiction" in Alberto Costi (ed) *Public International Law: A New Zealand Perspective* (LexisNexis NZ Ltd, Wellington, 2020) 361 at 361–362 and 368. See also PM *INTERPOL*, above n 35, at 24.

[37] SSA Report, above n 5, at [12.74]–[12.101]; and Costi, above n 36, at 386. See also Alan Toy "Cross-Border and Extraterritorial Application of New Zealand Data Protection Laws to Online Activity" (2010) 24 NZULR 222 at 225; and James Mullineux and Michelle Brown "The Authority for and Limits of Covert Investigation Methods in New Zealand" (2018) 28 NZULR 349 at 375–376.

[38] *Poynter v Commerce Commission* [2010] NZSC 38, [2010] 3 NZLR 300 at [30]–[31]; and *LM v R* [2014] NZSC 10, [2015] 1 NZLR 23 at [16]. See Chris Patterson "Remote Searching: Trawling in the Cloud" [2017] NZCLR 29 at 39. See also for example *Koppers Arch Wood Protection (NZ) Ltd v Commerce Commission* HC Auckland CIV-2004-404-3868, 16 November 2004.

[39] *Poynter*, above n 38, at [30]–[31].

[40] See *Ngapuhi*, above n 23, at [37]. See generally Patterson, above n 38, at 39.

[41] *R v Stevenson* [2012] NZCA 189, (2012) 25 CRNZ 755 at [57]; leave to appeal declined [2012] NZSC 63.

[42] David Harvey *internet.law.nz: selected issues* (Revised 4th ed, LexisNexis, Wellington, 2016) at [8.222]–[8.272]; and SSA Report, above n 5, at [14.151]–[14.155].

the United States,[43] will often refuse to comply with foreign requests on the basis that compliance would breach a "blocking statute", such as the United States Stored Communications Act (**SCA**).[44] The SCA ordinarily prohibits disclosure of communications content other than to United States law enforcement, but not other data,[45] although some service providers strictly refuse all foreign requests.[46] In recognition, while TICSA purports to impose its duty to assist with intercepts extraterritorially on overseas service providers operating in New Zealand,[47] it specifically preserves a common law defence potentially excusing assistance where complying would breach foreign law.[48]

B *MLA and "The MLAT Problem"*

MLA is the main tool law enforcement have to obtain and provide assistance in gathering overseas evidence for criminal investigations, operating through multilateral conventions, bilateral treaties (**MLATs**) and, absent those, principles of comity.[49] New Zealand's primary MLA statute, the Mutual Assistance in Criminal Matters Act 1992 (**MACMA**), regulates incoming requests from foreign states and outgoing requests by New Zealand.[50] While MACMA is not a code,[51] formal MLA requests under MACMA—rather than informal "police-to-police cooperation"[52]—are normally necessary to obtain communications content, because the requested state will typically use compulsory legal processes to obtain requested data.[53]

MLA is based on reciprocity: each state provides the level of assistance they expect to receive in return.[54] Requests are typically channelled through each state's 'central authority', responsible for reviewing and authorising requests.[55] New Zealand's central authority is formally the Attorney-General, but in practice MLA is administered by the Crown Law Office.[56] Crucially, incoming MLA requests are reviewed and executed in accordance with

---

[43] Andrew Keane Woods "Mutual Legal Assistance in the Digital Era" in David Gray and Stephen E Henderson (eds) *The Cambridge Handbook of Surveillance Law* (Cambridge University Press, Cambridge, 2017) 659 at 661.

[44] Woods, above n 43, at 662–663; and SSA Report, above n 5, at [14.155]. See generally *Controller & Auditor-General v Davison* [1996] 2 NZLR 278 (CA) at 327 and 342 per Richardson J; aff'd [1997] 1 NZLR 140 (PC).

[45] Woods, above n 43, at 662–663; and Stored Communications Act [**SCA**], 18 United States Code [**USC**] §§ 2702(a) and 2703(c).

[46] Woods, above n 43, at 663. See for example Google "Supplemental Submission on the Telecommunication (Interception Capability and Security) Bill" (12 July 2013) at [1.6].

[47] See TICSA, s 3(1) (definition of "service provider"); and above n 19.

[48] TICSA, s 28(8). Although described as an "absolute defence", (16 October 2013) 694 NZPD 13972, this merely preserves "the common law defence of foreign state compulsion", which applies a balancing test. See *Davison*, above n 44, at 291–292 per Cooke P, 327–331 per Richardson J, and 336–338 and 348–350 per Henry J.

[49] See Mutual Assistance in Criminal Matters Act 1992 [**MACMA**], ss 24–24B; Law Commission, *Modernising New Zealand's Extradition and Mutual Assistance Laws* (NZLC R137, February 2016) [**MLA Report**] at [3.1]; and *R v Bujak* [2007] NZCA 347 at [12]–[14]. See generally Boister, above n 1, at ch 18.

[50] See MACMA, Parts 2 and 3.

[51] At s 5; and for example *Bennett v District Court of New Zealand* [2021] NZHC 31 at [127]–[130].

[52] Boister, above n 1, at 311; and New Zealand Government, above n 1, at 2.

[53] Boister, above n 1, at 311; and PL *INTERPOL*, above n 35, at 24.

[54] Boister, above n 1, at 311; *R v Bujak*, above n 49, at [15] and [47]; *Solicitor-General v Bujak* [2008] NZCA 334, [2009] 1 NZLR 185 at [33]; and *Dotcom v Attorney-General* [2012] NZHC 1494, [2012] 3 NZLR 115 [***Dotcom (HC)***] at [32] (overruled on unrelated grounds).

[55] Boister, above n 1, at 313.

[56] MACMA, ss 8 and 25; MLA Report, above n 49, at [2.22] and [2.24]; and New Zealand Government, above n 1, at 2. For the Attorney-General's formal role, see *R v Bujak*, above n 49, at [18]. For the role of Crown Law

New Zealand law.[57] MLA is thus a "gateway", providing "foreign states with a route through which they can access the tools [the requested state] uses when investigating and prosecuting criminal activity".[58] Equally, the above—New Zealand's central authority, MACMA and other laws, and New Zealand courts—act as "gatekeepers" of individuals' rights, ensuring that New Zealand only provides MLA to foreign states consistently with New Zealand rights and values.[59]

MLA is however commonly viewed as "slow and cumbersome"[60]—a sentiment New Zealand courts share.[61] Electronic data requests are seen as particularly problematic, not least because the "un-territoriality" of data and evolving data storage methods make it difficult if not impossible to know where to direct requests.[62] The perceived ineffectiveness of MLA for overseas electronic data is so widely known that it is referred to generically as "the MLAT problem".[63] Various reforms and alternatives have been suggested.[64] These range from calls to better fund and modernise MLA, particularly in the United States[65]—the home of the largest global service providers and recipient of many incoming MLA requests for data[66]—through to entirely new proposals to bypass MLA entirely,[67] one of which is the CLOUD Act regime.

C *Digital Privacy: Section 21 and other mechanisms*

Rights generally are protected through *ex ante* and/or *ex post* mechanisms.[68] *Ex ante* protections, such as requiring independent approval of search warrants, are intended to minimise the likelihood of rights beaches.[69] *Ex post* tools, such as remedies for victims, address

---

Office, see *Commissioner of Police v Dotcom* [2012] NZHC 634 at [35]; and *Dotcom v Attorney-General* [2014] NZSC 199, [2015] 1 NZLR 745 [***Dotcom (SC)***] at [79].

[57] See Boister, above n 1, at 311; and MLA Report, above n 49, at [3.3].

[58] *Dotcom v Deputy Solicitor-General* [2015] NZHC 117, [2016] NZAR 229 at [20] (citing Law Commission *Extradition and Mutual Assistance in Criminal Matters* (NZLC IP37) [**MLA Issues Paper**] at [1.41]).

[59] MLA Issues Paper, above n 58, at [1.22] and ch 14; and MLA Report, above n 49, at 7 and ch 12.

[60] See MOJ and DPMC, *Consultation Paper: New Zealand accession to the Budapest Convention on Cybercrime* (July 2020) at [22].

[61] *R v Garcia* HC New Plymouth T/17/1, 5 November 2002 at [7]; *R v Fukushima* HC Auckland T032801, 30 April 2 04 at [105] and [109]–[110]; *Solicitor-General v Huanga (aka Wong)* HC Auckland CIV-2005-404-03, 9 Aust 2007 at [20]–[21]; *R v Bain* HC Christchurch CRI-207-412-000014, 5 March 2008 at [41]; *Solicitor-General v X* [2009] NZCA 476 at [24]–[27]; *AX (Permanent Resident)* [2018] NZIPT 204638 at [8]–[11]; *Commissioner of Police v Cheng* [2019] NZHC 2888 at [61]; *R v Cheng* [2020] NZHC 1861 at [16]; *R v Zagros* [2020] NZHC 1919 at [10]; and *R v Rodriguez* [2021] NZHC 425 at [24]–[25] and [45].

[62] See SSA Report, above n 49, at [2.67]. See generally Jennifer Daskal "The Un-Territoriality of Data" (2015) 125 Yale LJ 326.

[63] See for example Gail Kent 'The Mutual Legal Assistance Problem Explained" (23 February 2015) The Center for Internet and Society <http://cyberlaw.stanford.edu>; and Boister, above n 1, at 328.

[64] Woods, above n 35, at 663–673. See also SSA Report, above n 5, at [12.79]–[12.103] and [14.151]–[14.159].

[65] See Woods, above n 43, at 664–666.

[66] See 661–662.

[67] SSA Report, above n 5, at [14.151]–[14.159].

[68] Dimitrios Giannoulopoulos *Improperly Obtained Evidence in Anglo-American and Continental Law* (Hart Publishing, London, 2019) at 66 and 251–252. See also Andrew Geddis "The Comparative Irrelevance of the NZBORA to Legislative Practice" (2009) 23 NZULR 465 at 469–470, discussing *ex ante* and *ex post* rights protections within the Bill of Rights itself.

[69] See Giannoulopoulos, above n 68, at 251–252.

the impact of any breaches that nonetheless occur.[70] New Zealand provides relatively robust *ex ante* and *ex post* protections for privacy rights specifically. Privacy is protected in a "piecemeal" fashion,[71] including through the Privacy Act 2020, the common law,[72] and the New Zealand Bill of Rights Act 1990 (**Bill of Rights**), s 21 of which provides a right to be "secure against unreasonable search or seizure" by law enforcement and other public authorities.[73] Each privacy mechanism applies in the digital arena,[74] and there appears to be appetite to further develop them to respond to technological changes.[75]

Section 21 provides the "key protection" for privacy during law enforcement data collection.[76] It is "the closest [the Bill of Rights] comes to" a right to privacy.[77] "A touchstone of s 21 is the protection of reasonable expectations of privacy."[78] In this context, s 21 protects "a biographical core of personal information" people "wish to maintain and control from dissemination by the state."[79] Crucially, where law enforcement obtain evidence in breach of a defendant's reasonable expectations of privacy under s 21, the main protection is *ex post*,[80] through the exclusion of that evidence under s 30 of the Evidence Act, which sets out a two-part balancing test.[81] The greater the privacy intrusion, the more likely a court is to exclude.[82]

---

[70] At 251–252.

[71] Law Commission *Privacy: Concepts and Issues: Review of the Law of Privacy Stage 1* (NZLC SP19, January 2008) at [3.55]–[3.56]; and Paul Roth, "Privacy, Autonomy and Family Life" in Margaret Bedggood and others (eds) *International Human Rights Law in Aotearoa New Zealand* (Thomson Reuters, Wellington, 2017) 421 at 440. See also 440–449.

[72] *Hosking v Runting* [2005] 1 NZLR 1 (CA); and *C v Holland* [2012] NZHC 2155, [2012] 3 NZLR 672. See also *Driver v Radio New Zealand Ltd* [2019] NZHC 3275 at [137]. See generally Rosemary Tobin, "The Common Law Tort of Invasion of Privacy in New Zealand" in Stephen Penk and Rosemary Tobin (eds) *Privacy Law in New Zealand* (2nd ed, Thomson Reuters, Wellington, 2016) 89.

[73] See below nn 78–85.

[74] See (10 April 2018) 728 NZPD 3104 (Privacy Act 2020); *Henderson v Walker* [2019] NZHC 2184 at [217] (common law); and nn 87–89 (s 21). But see also *Graham v R* [2015] NZCA 568 at [26](c). See generally Law Commission *Review of the Privacy Act 1993: Review of the Law of Privacy – Stage 4* (NZLC R123, June 2011) at ch 10.

[75] See for example *Griffith v R* [2017] NZSC 61 at [3]; *R (SC 7/2020) v R* [2020] NZSC 51 at [23]; and *McIntyre v R* [2020] NZCA 503 at [40]. See generally Sian Elias, "Looking Back, Looking Forward: Reflections on 50 Years in the Law (2017) 23 Auckland U L Rev 14 at 28; and Helen Winkelmann, (then) Judge of the Court of Appeal of New Zealand, "Sir Bruce Slane Memorial Lecture" (November 2018) at 23.

[76] MLA Issues Paper, above n 58, at [17.94]. See also Dizon and others, above n 19, at 165–166.

[77] Roth, above n 71, at 440. The significance of the Bill of Right's omission of a free-standing right to privacy may be diminishing. See *D (SC 31/2019) v New Zealand Police* [2021] NZSC 2 at [92] per Winkelmann CJ and O'Regan J; and *Butland v R* [2019] NZCA 376 at [50]. See also Bill of Rights, s 28; and *Hosking v Runting*, above n 72, at [92].

[78] *R v Williams* [2007] NZCA 52, [2007] 3 NZLR 207 (CA) at [48] (citing *R v Fraser* [1997] 2 NZLR 442 (CA) at 449). See generally *Tupoumalohi*, above n 13, at [32]–[33].

[79] *Alsford*, above n 14, at [63]–[64] (quoting *R v Plant* [1993] 3 SCR 281 at 293).

[80] Andrew Butler and Petra Butler, *The New Zealand Bill of Rights Act: A Commentary* (2nd ed, LexisNexis NZ Ltd, Wellington, 2015) at [29.6.1]; and above n 76. See for example *Henderson v Attorney-General* [2017] NZHC 606, [2017] NZAR 707 at [81].

[81] *Hamed v R* [2011] NZSC 1, [2012] 2 NZLR 305 at [182]–[189] per Blanchard J; and *Reti*, above n 13, at [69]–[94].

[82] *Underwood v R* [2016] NZCA 312, [2017] 2 NZLR 433 at [21].

Other *ex post* privacy remedies, such as damages,[83] will typically be insufficient.[84] It is also only where privacy breaches trigger s 21 that exclusion appears available; merely breaching New Zealand's other main privacy mechanisms is apparently insufficient.[85] Section 21, and (for now) only s 21, therefore provides the greatest practical protection for privacy here.

Section 21's protections are vigorously applied in the digital arena as a consequence of the Supreme Court's December 2014 judgment *Dotcom v Attorney-General*.[86] The Court explained:[87]

> [S]earches of computers (including smart phones) raise special privacy concerns, because of the nature and extent of information that they hold, and which searchers must examine, if a search is to be effective. This may include information that users believe has been deleted from their files or information which they may be unaware was ever created. The potential for invasion of privacy in searches of computers is high….These are interests of the kind that s 21 of the Bill of Rights Act was intended to protect from unreasonable intrusion.

Following *Dotcom*, New Zealand courts are typically quick to recognise reasonable expectations of privacy under s 21 over various electronic data and devices,[88] including data transmitted through or held by service providers and other third parties.[89]

D *Rights protections during MLA*

Many jurisdictions, including the United States, United Kingdom, and Canada, provide significantly reduced protections for rights during MLA compared with domestic

---

[83] For other remedies, see Butler and Butler, above n 80, at [18.33] (Bill of Rights); Tobin, above n 72, at 109–110 (common law); and Privacy Act 2020, Pt 5.

[84] *R v Shaheed* [2002] 2 NLZR 377 (CA) at [24] per Elias CJ and [142], [148] and [153] per Richardson P, Blanchard and Tipping JJ; and *Hamed*, above n 81, at [70] per Elias CJ, [202] per Blanchard J, [247] per Tipping J, and [275] per McGrath J. See generally Andrew Ashworth, *Excluding Evidence as Protecting Rights* [1977] Crim L Rev 723.

[85] See *Alsford*, above n 14, at [47]; and *Graham*, above n 74, at [31]. But see also *Alsford*, above n 14, at [188] per Elias CJ dissenting; and Winkelmann, above n 75, at 19–20. New Zealand courts also have inherent jurisdiction to stay proceedings for rights breaches: *Wilson v R* [2015] NZSC 189, [2016] 1 NZLR 705 at [39]–[80].

[86] *Dotcom (SC)*, above n 56. For background, see Neil Boister "Law Enforcement Cooperation between New Zealana and the United States: Serving the Internet 'Pirate' Kim Dotcom Up on a 'Silver Platter'?" in Saskia Hufnagel and Carole McCartney (eds) *Trust in International Police and Justice Cooperation* (Oxford: Hart Publishing 2017) 193.

[87] *Dotcom (SC)*, above n 56, at [191]. See also [57] per Elias CJ dissenting (but not on that point).

[88] *Makaea v R* [2018] NZCA 284 at [39] and [45]; and *Tupoumalohi*, above n 13, at [34] and [39]. See for example *R v Lucas* [2015] NZHC 1944 at [41]; *McLean v R* [2015] NZCA 101 at [27]; *Murray v R* [2016] NZCA 221 at [168]; *R v Trethewey* [2016] NZDC 8957, [2018] DCR 425 at [34]; *W (CA597/2016)*, above n 12, [29]–[30] and [34]; *Henderson*, above n 80, at [44]–[45]; *Fenwick*, above n 10, at [41](a); *Wikitera v Ministry for Primary Industries* [2018] NZCA 195, [2018] 3 NZLR 770 at [15], [38], and [45]; *Hogg*, above n 23, at [40]; and *Jeffries v Ministry of Social Development* [2020] NZHC 1450 at [45]. For judgments prior to *Dotcom (SC)*, see for example *McGaughey v R* CA269/07, 17 September 2007 at [17]; *Bogue*, above n 10, at [66]–[67]; and *Hoete*, above n 10, at [36]. But see also for example *S (CA712/2015) v R* [2016] NZCA 448 at [41]–[45]; and *Wilkie v R* [2019] NZCA 62 at [32].

[89] See for example *Murray*, above n 88, at [168]; *Fenwick*, above n 10, at [32]–[41](a); and *Reti*, above n 13, at [75]–[79]. See generally Butler and Butler, above n 79, at [18.14.9]–[18.14.13] and [18.14.40]; and *Alsford*, above n 14, at [55]–[65].

investigations.[90] In contrast, although MAMCA is "complex and convoluted",[91] New Zealand courts typically ensure that it is interpreted and applied consistently with the Bill of Rights,[92] including s 21 specifically.[93] These and other gatekeepers provide credible rights protections, whether New Zealand is *requesting* MLA or being *requested* to provide it, at each stage at which rights may be impacted: making an MLA request; its execution in the requested state; and the use of MLA evidence in criminal proceedings in the original requesting state.[94]

As a requesting state, all of New Zealand's MLA conduct, including initial acts seeking MLA, may be subject to judicial scrutiny and must comply with the Bill of Rights.[95] New Zealand cannot control how its MLA requests are executed overseas, creating the scope for protection gaps for rights relative to domestic evidence collection.[96] However, Blanchard J has suggested that the Bill of Rights "at least" requires New Zealand to ask that evidence be gathered overseas in a particular way.[97] When New Zealand seeks to rely on MLA evidence in criminal proceedings, its admissibility will be subject to standard evidential rules.[98] In particular, courts will exclude MLA evidence where its admission would breach the Bill of Rights.[99] Although courts may presume that MLA evidence has been obtained in accordance with foreign law[100]—again risking protection gaps—this presumption appears rebuttable.[101]

As a requested state, New Zealand's role is more limited, comprising reviewing and executing a request and transmitting evidence overseas.[102] There is, again, scope for protection gaps: courts presume foreign states have acted lawfully and reasonably in making MLA

---

[90] For the United States and United Kingdom, see Cochrane, above n 9, at 24–35, 39–45, and 50–52. For Canada, see Robert J Currie '*Charter* Without Borders? The Supreme Court of Canada, Transnational Crime and Constitutional Rights and Freedoms' (2004) 24 Dalhousie LJ 335 at 272–281; *R v Hape* 2007 SCC 26, [2007] 2 SCR 292; and for example *R v F (JM)* 2018 MBQB 156.

[91] MLA Issues Paper, above n 58, at [1.7].

[92] *Samleung International Trading Co Ltd v Collector of Customs* [1994] 3 NZLR 284 (HC) at 289–291; *R v Bechmann-Hansen* [1997] 1 NZLR 598 (HC) at 609–611; *R v Gummer* [2002] DCR 425 at [18](v); *R v Connelly* [2004] 3 NZLR 794 (HC) at [16]–[17] and [67]; and *Dotcom (SC)* at [100]–[103] and [161]–[162]. See also *A v District Court at Auckland* HC Auckland CIV-2011-404-4796, 22 December 2011 [***A (HC)***] at [58]; aff'd [2012] NZCA 246, [2012] 2 NZLR 844 [***A (CA)***]. See generally Bill of Rights, ss 5 and 6.

[93] *Avowal Administrative Attorneys Ltd v District Court at North Shore* [2012] NZCA 183, [2010] 4 NZLR 661 at [22]; *Dotcom (SC)*, above n 56, at [10] per Elias CJ dissenting (but not on this point) and [100] and [161] per McGrath and Arnold JJ. See also *X v Refugee Status Appeals Authority* [2006] NZAR 533 (HC) at [55] and [59]–[66].

[94] See Cochrane, above n 9, at 24.

[95] See for example *Bechmann-Hansen*, above n 92; and *Civil Aviation Authority of New Zealand v Heavylift Cargo Airlines Pty Ltd* [2008] NZCA 76, [2008] 3 NZLR 391. See generally MLA Issues Paper, above n 58, at ch 12.

[96] *Bechmann-Hansen*, above n 92, at 610–611.

[97] At 610–611. See also *Connelly*, above n 92, at [68].

[98] MACMA, s 63; and *Connelly*, above n 92, at [49].

[99] *Bechmann-Hansen*, above n 92, at 609–611; *Gummer*, above n 92, at [21]–[22] and [39]; and *R v Robinson* [2016] NZHC 179 at [45 –[46]. See also *Connelly*, above n 92, at [125].

[100] See for example *Heavylift*, above n 95, at [33]–[34].

[101] See *Financial Markets Authority v Lacy* [2015] NZHC 1114 at [37]. See also SSA Report, above n 5, at [12.143]; and Harvey, above n 42, at [8.260].

[102] See *Dotcom (SC)*, above n 56, at [26] per Elias CJ dissenting (but not on this point). See generally MLA Issues Paper, above n 58, at ch 12, 14–15 and 17.

requests,[103] and may take on trust information supplied in support.[104] It has also been suggested that New Zealand should not be concerned with how evidence provided will be used by the requesting state.[105] Courts justify these approaches in part by noting that New Zealand's central authority will presumably already have reviewed MLA requests.[106] In any event, New Zealand's own acts executing foreign MLA requests must again strictly comply with MACMA and the Bill of Rights.[107] Where New Zealand uses compulsory processes to obtain evidence for a foreign state, its acts must meet at least the same standards that apply during domestic investigations.[108]

Dotcom offers particular guidance for protecting rights when New Zealand acts as a requested state. Addressing the validity of a search warrant issued under MACMA at the request of the United States,[109] *Dotcom* emphasised that cross-border contexts like MLA require *enhanced* protections: in particular, the court held that:[110]

> [T]hose who wish to challenge the legality of searches conducted under [MLA] search warrants need timely access to the High Court to challenge by judicial review what was done before what is seized is sent overseas to the authorities of the requesting country.

Challenges should be permitted by underlying targets, as well as providers and others significantly affected, who may vicariously assert targets' privacy rights.[111] The Supreme Court's comments should also apply equally to other compulsory processes, such as production orders.[112] While compulsory powers to obtain data are invariably sought on a without notice basis,[113] and although judicial review of such investigative steps is ordinarily rare,[114] both the current and former Chief Justices have explained that New Zealand courts, as MLA

---

[103] *Bujak*, above n 54, at [22](a) and [33]–[36]; *Re Keen* [2013] NZHC 2382; and *Chatfield & Co Ltd v Commissioner of Inland Revenue* [2016] NZHC 1234, (2016) 27 NZTC 22–053 at [14]–[21] (citing *Abu v Comptroller of Income Tax* [2015] SGCA 4, [2015] 2 SLR 420). See for example *Re Stewart* HC Wellington M93/96, 10 September 1996 at 7; *Webb Ross Johnson v District Court at Whangarei* HC Whangarei CP.1/99, 5 February 1999 at 6; and *A (HC)*, above n 92, at [76]–[77], aff'd *A (CA)*, above n 92, at [64]–[66].

[104] *A (CA)*, above n 92, at [32]–[41].

[105] *Re Rutherford and the Princely Court of Justice, Liechtenstein* [2001] NZAR 338 (HC) at [17].

[106] At [16]; and *A (CA)*, above n 92, at [42].

[107] *Dotcom (HC)*, above n 54, at [33] (overruled on other grounds). See also *A (CA)*, above n 92, at [40]; and *Chatfield & Co Ltd v Commissioner of Inland Revenue* [2017] NZHC 3289, [2018] 2 NZLR 835 [40]–[41], [47]–[48] and [78], aff'd [2019] NZCA 73, [2019] 2 NZLR 832 at [40]–[44]; aff'd [2019] NZSC 84, (2019) 29 NZTC 24–016 at [7].

[108] *Webb Ross Johnson*, above n 103 at 7; *Dotcom (HC)*, above n 54, at [35] (overruled on other grounds); and *A (HC)*, above n 92, at [59].

[109] *Dotcom (SC)*, above n 56, at [68]–[88]. Its findings are not limited to MACMA. See *Hager v Attorney-General* [2015] NZHC 3268, [2016] 2 NZLR 523 at [139] n 60.

[110] *Dotcom (SC)*, above n 56, at [199]–[200]. See also [26] and [46] per Elias CJ dissenting but not on this point; and MLA Issues Paper, above n 58, at [17.94]–[17.96].

[111] See for example *X v Hastings District Court* HC Napier CIV-2004-441-93, 16 December 2004 at [70] and [84]–[93]; and *Calver v District Court at Palmerston North (No 1)* [2005] DCR 114 (HC) [75]–[83] and [86]. See generally Philip A Joseph *Constitutional and Administrative Law in New Zealand* (Wellington: Thomson Reuters, 2014) at [2.27.6.3](1).

[112] See SSA Review, above n 5, at [14.02]; and *Alsford*, above n 14, at [18]–[20].

[113] *Reti*, above n 13, at [40].

[114] *Singh v Chief Executive of the Ministry of Business, Innovation and Employment* [2014] NZCA 220, [2014] 3 NZLR 23 at [38]–[39].

gatekeepers, should entertain judicial review in this context because once material is transferred overseas New Zealand loses control.[115] There is a real risk that, if rights are not protected in New Zealand, they will not be protected at all.[116]

III The CLOUD Act Regime[117]

A *Background*

In 2015 the United Kingdom's "Special Envoy on intelligence and law enforcement data sharing", Sir Nigel Sheinwald, reported back after discussions with law enforcement and service providers on how to address the MLAT problem.[118] Although Sir Nigel recommended reforming MLA, he considered it would "never be fast enough or have a scope wide enough" to resolve the MLAT problem.[119] He suggested a "sustainable and longer-term solution" would instead be to "allow 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 the companies."[120] These recommendations were accepted by the United Kingdom, which began negotiating the US-UK Agreement that same year.[121]

During the same period, the United States and United Kingdom were also conducting "unilateral assertions of extraterritorial authority",[122] seeking to bypass MLA by directly enforcing their own laws overseas. The most famous United States attempt was considered by a Second Circuit Court of Appeals panel in *Microsoft Ireland* in 2016.[123] It ruled that using the SCA to compel disclosure of data stored by Microsoft in an Irish data centre would be an impermissible extraterritorial use of that legislation, contrary to its underlying privacy focus.[124] Although *Microsoft Ireland* was appealed—ultimately to the United States Supreme Court, which heard oral argument in February 2018—on 23 March 2018, Congress passed the CLOUD Act, rendering the appeal moot.[125] The United Kingdom, which passed companion

---

[115] *Dotcom (HC)*, above n 54, at [33]–[35] per Winkelmann J (as she then was) (overruled on other grounds); and *Dotcom (SC)*, above n 56, at [26] and [46] per Elias CJ (dissenting but not on this point). See *Dotcom v Attorney-General* [2014] NZCA 19, [2014] 2 NZLR 629 [***Dotcom (CA)***] at [101]; *Chatfield & Co Ltd v Commissioner of Inland Revenue* [2015] NZHC 2099, (2015) 27 NZTC 22–024 at [38] n 10; and MLA Issues Paper, above n 58, at [17.94]–[17.96]. Contrast *Southern Storm (2007) Ltd v Chief Executive, Ministry of Fisheries* [2013] NZHC 117 at [58].

[116] See above n 90.

[117] See Cochrane, above n 9, at 11–15 for more detailed analysis of the first three subsections below.

[118] *Summary of the Work of the Prime Minister's Special Envoy on Intelligence and Law Enforcement Data Sharing – Sir Nigel Sheinwald* (25 June 2015) at 1.

[119] At 2.

[120] At 2. See also Nicola Newsom *Crime (Overseas Production Orders) Bill [HL]: Briefing for Lords Stages* (House of Lords Library Briefing Paper, 5 July 2018) at 2–7.

[121] Newsom, above n 120, at 5.

[122] Jennifer Daskal *Law Enforcement Access to Data Across Borders: the Evolving Security and Rights Issues* (2016) 8 J Nat Secy L & Poly 473 at 477–478.

[123] *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 generally Justin Hemmings, Sreenidhi Srinivasan and Peter Swire *Defining the Scope of "Possession, Custody, or Control" for Privacy Issues and the CLOUD Act* (2010) J Natl Secy L & Poly 631 at 646–652.

[124] *Microsoft Ireland*, above n 123, at 216–21.

[125] See Hemmings, Srinivasan and Swire, above n 123, at 651–652.

legislation the following year, the Crime (Overseas Production Orders) Act 2019 (**COPOA**),[126] initially had greater success at applying Serious Fraud Office statutory information-gathering powers extraterritorially.[127] In February 2021, however, its Supreme Court issued *KBR*, holding that it was "inherently improbable" that these powers were intended to apply extraterritorially, noting "successive Acts of Parliament" instead demonstrated a Parliamentary preference for MLA.[128]

The US-UK Agreement itself was signed in September 2019.[129] Although subject to negative resolution periods before Congress and the United Kingdom Parliament,[130] these have now elapsed. It may now be brought into force at any point through an exchange of diplomatic notes[131]—a process yet to occur.

B *Operation*

The CLOUD Act has two main parts. First, it introduced a new SCA section expressly permitting orders to compel data within the "possession, custody or control" of a company subject to United States jurisdiction, regardless of the data's location.[132] Secondly, it enabled the CLOUD Act regime, creating a United States mechanism for bilateral agreements with foreign states to facilitate cross-border law enforcement data access.[133]

Like MLA, the CLOUD Act regime is based on reciprocity.[134] However, requests for data will now be made directly to overseas service providers under the law of the requesting state, bypassing MLA.[135] Central authorities have significantly reduced roles: they will normally only be involved in outgoing requests; their "supervisory role" over incoming requests has been removed.[136] Under the US-UK Agreement, providers may be compelled not only to preserve or disclose data but also to intercept live data[137]—going significantly beyond existing US-UK MLA.[138]

A "core obligation" is that each state agrees to suspend 'blocking statutes' that would otherwise prohibit service providers in their jurisdiction from responding directly to requests from the other state.[139] In that sense, the regime is permissive—United States law, for example,

---

[126] See Newsom, above n 120, at 10.

[127] *R (KBR, Inc) v Dir of the Serious Fraud Office* [2018] EWHC (Admin) 2368 [63]–[78], [2019] QB 675. See generally Alex Davidson "Extraterritoriality and statutory interpretation: the increasing reach of investigative powers" [2020] Pub L 1.

[128] *R (KBR Inc) v Director of the Serious Fraud Office* [2021] UKSC 2, [2021] 2 WLR 335 at [45].

[129] US-UK Agreement, above n 3, at 17; and USDOJ, above n 2.

[130] See Crime (Overseas Production Orders) Act 2019 (UK) [**COPOA**], s 1(6); and CLOUD Act, § 105(a) (codified at 18 USC § 2523(d)).

[131] US-UK Agreement, above n 3, at art 15.

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

[133] At § 105(a) (codified at 18 USC § 2523(d)).

[134] CLOUD Act, § 105 (codified at 18 U.S.C. 2523(b)(4)(i)); and US-UK Agreement, above n 3, at art 3(b).

[135] See US-UK Agreement, above n 3, at arts 3(1)–(2), 5(1)–(2), and 10(1)–(2). See also arts 8(1), 9(2), and 10(5).

[136] See arts 5(5)–(9), 6(1)–(2), and 10(2).

[137] See arts 1(11) and 5(3).

[138] See United Kingdom Home Office *Requests for Mutual Legal Assistance in Criminal Matters: Guidelines for Authorities Outside of the United Kingdom* (12th ed, 2015) at 30.

[139] (20 November 2018) 794 GBPD HL 139–140. See *US White Paper*, above n 4, at 4; and UKFCO *Explanatory Memorandum to the Agreement Between the Government of the United Kingdom of Great Britain and Northern*

will merely *allow*, but not *require*, its service providers to respond to United Kingdom requests under the US-UK Agreement. However, it is "premised on the notion" that members "have the authority under their domestic laws to compel production of data held abroad"[140]—and United States providers who refuse to comply with United Kingdom requests may face contempt of court there and potentially worse.[141] While enforcing compulsory law enforcement requests overseas *unilaterally* risks beaching customary international law,[142] such enforcement may be entirely lawful where the sovereign state of that foreign territory consents.[143] The US-UK Agreement seeks to provide such consent: it allows each state to expand enforcement jurisdiction against overseas providers previously "beyond the reach of existing domestic court orders".[144]

The United Kingdom's approach provides guidance on implementation. Its Investigatory Powers Act 2016 (**IPA**) ordinarily functions as a blocking statute, making it unlawful for United Kingdom service providers to respond directly to many foreign law enforcement requests.[145] To lift this, the UK designated the US-UK Agreement under s 52 of the IPA:[146] this authorises service providers intercepting—or disclosing[147]—data in response to a request made "in accordance with a [designated] international agreement by the competent authorities of a country or territory outside the United Kingdom".[148] Such requests become lawful not only under the IPA but "for all other purposes" under UK law.[149] The United Kingdom also enacted COPOA to provide a new mechanism to compel stored data from overseas providers, so long as, similarly, requests are made under a designated international agreement such as the US-UK Agreement.[150] COPOA's powers complement existing IPA powers purporting to compel extraterritorial intercepts[151]—powers given practical force by the US-UK Agreement.[152]

C *Rights protections*

Before a country may obtain a CLOUD Act agreement with the United States, the United States Attorney-General must certify that the country provides sufficient domestic law protections for

---

Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime (2019) [***UK Explanatory Memorandum***] at [8].

[140] *US White Paper*, above n 4, at 4–6 and 14; and *UK Explanatory Memorandum*, above n 139, at [7].

[141] Contempt is the penalty under COPOA. See Criminal Procedure Rules 2020 (UK), r 47.71. Additional penalties apply under the Investigatory Powers Act 2016 (UK) [**IPA**].

[142] See nn 36–37.

[143] Costi, above n 36, at 368.

[144] COPOA, Explanatory Notes at [2]–[5]. See also Jennifer Daskal, *Transnational Government Hacking* (2020) 10 J Natl Secy Law Poly 677 at 695.

[145] See IPA, ss 3 and 11; and (20 November 2018) 794 GBPD HL 139–140.

[146] The Overseas Production Orders and Requests for Interception (Designation of Agreement) Regulations 2020 (UK) [**Designation Regulations**] , reg. 2(b).

[147] IPA, ss 4 and 52; and (20 November 2018) 794 GBPD HL 140–141.

[148] IPA, s 52(3).

[149] At s 6. See *In re McE* [2009] UKHL 15, [2009] 1 AC 908 at [61]. But see also [74].

[150] See COPOA, ss 1 and 4; and Designation Regulations, reg 2(a).

[151] IPA, ss 15(1)(b), (3), (5), and 41–43.

[152] See David Anderson *A Question of Trust: Report of the Investigatory Powers Review* (UK Independent Reviewer of Terrorism Legislation, June 2021) at [6.99] and [11.17]–[11.24].

rights.[153] Further *ex ante* protections apply under the US-UK Agreement: states agree to comply with their own digital privacy laws;[154] to engage in periodic reviews of their compliance and data handling;[155] and to apply the protections of the EU-US 'Umbrella Agreement', which mandates safeguards for data transmitted for law enforcement purposes between its signatories.[156] In the United States, the Umbrella Agreement's obligations are implemented by extending the protections of the Privacy Act of 1974—a "narrowly tailored" statute[157]—to UK persons through designations under the Judicial Redress Act.[158]

Targeting and minimization procedures also apply.[159] Each state may target their own or third country nationals (**TCNs**) but normally not nationals of the other state or indeed anyone "located in" the other state.[160] This is, however, only semi-reciprocal: while the United Kingdom is always prohibited from targeting United States persons, the United States is restricted from targeting United Kingdom persons only while they are physically within United Kingdom territory.[161]

The main *ex post* protection is the service providers, who may object if they believe a request is improper.[162] This request must initially be made to the requesting state, but may ultimately be escalated to, and resolved by, the providers' own state.[163] Other than this, however, a providers' own state will normally have no involvement in, or even knowledge of, requests.[164] When TCNs are targeted, a default obligation to notify authorities in the TCNs' state also applies.[165]

D *A US-NZ CLOUD Act Agreement*

A US-NZ Agreement—assumedly similar to the US-UK Agreement—would be a bilateral international treaty,[166] thus subject to New Zealand's treaty-making requirements.[167] It would likely be materially novel and thus a "major bilateral treaty of particular significance",

[153] CLOUD Act, § 105(a) (codified at 18 USC § 2523(b)(1)).

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

[155] US-UK Agreement, above n 3, at art 12(1).

[156] At arts 9(1) and 10(9); and Agreement Regarding Law Enforcement Exchange and Protection of Information, United States – European Union TIAS 17-201 (signed 2 June 2016, entered into force 1 February 2017).

[157] United States House of Representatives *Judicial Redress Act of 2015* (Report 114 -294, 2015) at 3–4.

[158] "Attorney General Designations" (12 February 2019) 84 *Fed Reg* 3493.

[159] At arts 4 and 7.

[160] See art 1(12) and 4(3).

[161] At arts 1(12), 4(3). See *UK Explanatory Memorandum*, above n 139, at [7].

[162] U.S.-U.K. Agreement, above n 3, at arts 5(11)–(12).

[163] At art 5(12).

[164] See Andrew Smith "Overseas Production Orders: Getting Up to Speed" (2019) 169(7830) New LJ 9 at 9.

[165] US-UK Agreement, above n 3, at art 5(10). But see Cochrane, above n 9, at 53.

[166] Theodore Christakis and Kenneth Propp "The Legal Nature of the US-UK CLOUD Agreement" (20 April 2020) Cross-Border Data Forum <www.crossborderdataforum.org>.

[167] Cabinet office *Cabinet Office Manual 2017* at [5.77]–[5.81]; and MFAT, above n 8.

requiring a National Interest Analysis,[168] as well as Parliamentary scrutiny of both the US-NZ Agreement and the bill implementing New Zealand domestic law changes.[169]

Legislative amendments, ideally to the SSA,[170] would be necessary to ensure New Zealand could directly compel United States service providers to preserve, disclose, and intercept data under New Zealand law. As the CLOUD Act regime is for law enforcement,[171] this article assumes equivalent intelligence-gathering powers are outside its scope.[172] SSA amendments required include new "extraterritorial production orders", presumably similar to existing production orders, albeit expressly extraterritorial.[173] Similar amendments to SSA intercept powers would likely be required: although New Zealand asserts existing powers already have some extraterritorial reach,[174] their precise scope is unclear but in any event appears significantly more limited than permitted under a US-NZ Agreement.[175] Comparable changes may be required for SSA preservation powers New Zealand plans to shortly enact.[176] Any new extraterritorial powers should be exercisable only in accordance with a 'designated international agreement', to reduce comity concerns,[177] as well as to facilitate future agreements.[178]

New Zealand would also need a legislative mechanism to lift blocking statutes that may currently prohibit its own service providers from responding directly to United States requests under a US-NZ Agreement.[179] The Crimes Act 1961 criminalises *intercepting* private communications, unless party to the communications or authorised under the SSA or similar authority, as well as disclosing intercept product.[180] These offences apply to New Zealand

---

[168] Cabinet office *Cabinet Office Manual* 2017 at [7.123]–[7.133]; MFAT, above n 167, at 15; and Standing Orders of the House of Representatives 2020, SO 254(2) and 405–408. See also Treasa Dunworth "International Law in New Zealand Law" in Alberto Costi (ed) *Public International Law: A New Zealand Perspective* (LexisNexis NZ Ltd, Wellington, 2020) 597 at 605–613.

[169] See also Cabinet Office *Cabinet Manual 2017* at [5.79]; and MFAT, above n 167, at 7.

[170] See generally Butler and Butler, above n 80, at [18.4.1]; and *Cullen v District Court* [2017] NZHC 486 at [41]–[43].

[171] US-UK Agreement, above n 3, at Preamble and art 2(1); and 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* (Cambridge University Press, Cambridge, 2020) 319 at 335.

[172] See Intelligence and Security Act 2017; and Mullineux and Brown, above n 37, at 380 n 161. There may however be blurring with intelligence gathering when investigating "terrorist activity". See US-UK Agreement, above n 3, at Preamble and art 2(5); and Gehan Gunasekara 'The "Final Privacy Frontier? Regulating Trans-Border Data Flows' (2007) 17 Intl J L & Info Tech 147 at 169.

[173] SSA Report, above n 5, at [14.159].

[174] See above nn 47–48.

[175] Above n 18. See Ben Keith "Official access to encrypted communications in New Zealand: Not more powers but more principle?" [2020] Common Market L Rev 1 at 13–14. See also SSA Report, above n 5, at [9.5]; and Dizon and others, above n 19, at 76–77.

[176] See Cabinet Office, above n 14, at [41]–[53].

[177] See generally *Poynter*, above n 38, at [30](b), [37], and [43].

[178] See for example COPOA, ss 1(2) and (5), 4(2); and Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (Australia) [**TLAIPOA]**, Sch 1, Pt 1, cls 21.

[179] See Google, above n 46, at [3.8], offering similar analysis.

[180] Crimes Act 1961, ss 216B–216C. See also ss 26(3) and 28.

service providers.[181] *Accessing* and disclosing equivalent stored data may similarly be a criminal offence, although this is less clear[182]—the Law Commission has therefore recommended a bespoke offence.[183] Information Privacy Principle [**IPP**] 11 within the Privacy Act 2020 also prohibits the disclosure of personal information except in certain specific circumstances,[184] as does an equivalent code for telecommunication service providers specifically.[185] Additional restrictions now normally apply where information is being disclosed overseas under new IPP12.[186] How these and related provisions would apply here is fact-dependent and ultimately beyond the scope of this article.[187] It would in any event be necessary to legislate exceptions from these specific statutes to provide comfort to providers.[188] These should similarly be triggered only by requests made under a 'designated international agreements'.

IV Advantages and Risks for New Zealand

A *Faster access to overseas data*

A US-NZ Agreement would likely significantly speed up New Zealand law enforcement's access to data held by overseas service providers relative to MLA. The United Kingdom estimates that the COPOA procedure will reduce the average time it takes to obtain stored data from United States service providers from one year[189]—with some requests taking significantly longer[190]—down to "60 days and perhaps less".[191] Although concerns have been raised about the ability to practically enforce such requests overseas[192]—already an issue of concern for New Zealand[193]—the main global service providers, likely to be on the receiving end of most requests,[194] support the regime.[195] Given the growing importance of electronic data for New

---

[181] See s 16A and 216B(5); Law Commission *Invasion of Privacy: Penalties and Remedies: Review of the Law of Privacy – Stage 3* (NZLC R113, January 2011) at 111; and *Adams on Criminal law* (online loose-leaf ed, Thomson Reuters) at [CA216A.01] (citing *McFall*, above n 10, at [52]).

[182] See Crimes Act 1961, s 249. See also ss 217 and 248; *Watchcorn v R* [2014] NZCA 493 at [68]–[81]; and *Adams on Criminal Law*, above n 181, at [CA217.02] and [CA249].

[183] Law Commission, above n 181, at 110–111.

[184] Privacy Act 2020, s 22, Information Privacy Principle [**IPP**] 11.

[185] Telecommunications Information Privacy Code 2020 [**TIPC**], cl 6, r 11.

[186] See Privacy Commissioner *Disclosing personal information outside New Zealand – the new information privacy principle 12* (December 2020). See also Privacy Act 2020, s 22, IPP12(2); and TIPC, cl 6, r 12(2).

[187] See for example Privacy Act 2020, ss 4, 11, 22, IPP11(2), and 23. See generally *Green v EIT* [2020] NZHRRT 24 at [126].

[188] See for example TLAIPOA, Sch 1, Pt 1, cls 167–169. Contrast n 149 above. See also Privacy Act 2020, s 24(1).

[189] *UK Explanatory Memorandum*, above n 139, at [2].

[190] At [2].

[191] United Kingdom Home Office, *Impact Assessment: Police, Crime, Sentencing and Courts Bill* (HO0383, 23 February 2021) at 6. See also COPOA, s 5(5).

[192] See for example Smith, above n 164, at 10. See generally above n 140.

[193] See for example Office of the Privacy Commissioner "Privacy Commissioner: Facebook must comply with NZ Privacy Act" (28 March 2018) <www.privacy.org.nz>. See generally SSA Report, above n 5, at [14.153].

[194] See SSA Report, above n 5, at [12.102].

[195] Cabinet Office, above n 14, at [17]. See for example Letter from Apple, Facebook, Google, Microsoft and Oath to Orrin Hatch and others (US Senators) regarding CLOUD Act (6 February 2018),

Zealand criminal investigations, the potential for much quicker access to overseas data under a US-NZ Agreement appears significant.

B *Other potential benefits*

Requests by New Zealand for overseas data may also have fewer 'protection gaps' for rights than MLA. Protection gaps arise under MLA because New Zealand must trust on a foreign requested state to obtain requested evidence in a rights-compliant manner and may have limited ability to verify this.[196] Under a US-NZ Agreement, New Zealand would normally control the entire evidence-gathering process when it requests data.[197] New Zealand law enforcement will therefore be better placed to ensure that this process complies with rights, as will New Zealand courts to exercise judicial oversight. However, the CLOUD Act regime permits requests to be made with very few safeguards—notably, prior judicial authorisation is not required.[198] Although this article recommends that New Zealand legislates new regime powers within the SSA, it might instead use alternative mechanisms, with limited safeguards and thus additional protection gaps. Such unregulated searches and seizures may ordinarily breach s 21,[199] subject to expressly contrary legislation.[200] However, executing regime requests overseas would likely be "extraterritorial" under New Zealand law,[201] and whether the Bill of Rights applies to such extraterritorial conduct is "yet to be authoritatively explored."[202] Absent this, or a New Zealand commitment to legislative regime powers within the SSA or equivalent legislation,[203] this second benefit remains merely potential.

A further theoretical claimed advantage is that, if New Zealand were a CLOUD Act regime member, service providers could use a special new comity defence to object to United States SCA requests for the data of overseas persons where complying would generate a New Zealand law conflict.[204] However, assuming such SCA requests were also channelled through a US-NZ Agreement, New Zealand law conflicts would be unlikely—its blocking statues would be lifted and thus inapplicable.[205] United States law, like New Zealand,[206] also already

---

<https://blogs.microsoft.com>; and Microsoft "Submission to public consultation on a proposal for New Zealand to join the Budapest Convention" (11 September 2020) (Obtained under OIA request to MOJ) at 3.

[196] See text accompanying above nn 95–101.

[197] See text accompanying above nn 135–136 and 164.

[198] CLOUD Act, § 105(a) (codified at 18 USC § 2523(b)(4)(D)); and US-UK Agreement, *supra* note 3, at arts. 1(11), 5(1)–(2), 55(5)–(7), and 10(2).

[199] See *Alsford*, above n 14, at [35] and [47].

[200] See Bill of Rights, s 4. See for example Child Protection (Child Sex Offender Government Agency Registration) Amendment Act 2021, s 5(7).

[201] SSA Report, above n 5, at [14.151]–[14.159]; and above nn 40–38. See also Alan Toy and Gehan Gunasekara "Is There a Better Option Than the Data Transfer Model to Protect Data Privacy?" (2019) 42 UNSW LJ 719 at 721.

[202] *Smith v R* [2020] NZCA 499 at [92]. See also *Young v Attorney-General* [2018] NZCA 307, [2018] 3 NZLR 827 at [40]. See generally Butler and Butler, above n 80, at [5.16].

[203] See SSA, s 5; and *Roskam v R* [2019] NZCA 53 at [19].

[204] CLOUD Act, § 103(b) (codified at 18 USC § 2703(h)).

[205] See *US White Paper*, above n 4, at 14.

[206] Above n 48.

recognises a common law comity defence.[207] It is far from clear that this new statutory test would provide greater protections.[208]

C *Risks to Digital Privacy*

New Zealand gatekeepers protect rights when foreign states request MLA.[209] In an extensive review of MLA,[210] the Law Commission recommended expanding and strengthening these safeguards, particularly the role of New Zealand's central authority,[211] which it considered "the key to ensuring" rights "are sufficiently protected".[212] It was strongly critical of allowing foreign states any ability to directly compel disclosure or interception of New Zealand data.[213] Yet the reciprocal nature of the CLOUD Act regime—requiring New Zealand to permit the United States to compel New Zealand service providers to preserve, disclosure, or intercept data without local oversight—would almost entirely remove these gatekeepers,[214] leaving requests regulated solely by United States law.

United States law would however provide much more limited protections for the digital privacy of New Zealand persons and TCNs compared to US-NZ MLA.[215] Consider first the evidence-gathering process itself. Assuming United States requests under a US-NZ Agreement were made through mechanisms like the SCA,[216] some *ex ante* safeguards would apply—notably, requests for communications content require prior judicial authorisation based on 'probable cause'.[217] *Ex post* protections would however be significantly reduced: while both targets and service providers may challenge MLA in New Zealand courts on rights grounds,[218] targets apparently lack standing to oppose SCA orders during evidence-gathering,[219] and providers are traditionally barred from vicariously asserting targets' rights during SCA challenges.[220] Even if providers—now the main gatekeepers of targets' rights under the CLOUD Act regime—can now permissibly raise these objections directly under a US-NZ

---

[207] *Societe Nationale Industrielle Aerospatiele v US Dist Court for S. Dist. of Iowa* 482 US 522 (1987) at 544 and 544 n 29. See CLOUD Act, § 103.

[208] See Cochrane, above n 9, at 48 n 370.

[209] See above n 59.

[210] See generally MLA Issues Paper, above n 58; and MLA report, above n 49.

[211] MLA report, above n 49, at 7, ch 2, and [12.4].

[212] At [12.5]. See also Law Commission *The Use of DNA in Criminal Investigations* (NZLC R144, October 2020) [**DNA Report**] at [23.55], [23.60], [23.61], and [23.79], reiterating these views.

[213] MLA Issues Paper, above n 58, at [17.34], [17.68], and [17.70].

[214] See text accompanying above n 163.

[215] The rights of United States persons, in contrast, would likely be enhanced, as the "international silver platter doctrine" should no longer apply. See Cochrane, above n 9, at 35–39 and 52–53. See also Boister, above n 86, at 214.

[216] The United States may arguably also issue CLOUD Act regime requests using alternative mechanisms with fewer safeguards. See text accompanying above nn 198–202; and Cochrane, above n 9, at 37–38.

[217] Cochrane, above n 9, at 32 n 225 and 40–41. On probable cause, see *Hamed*, above n 81, at [144] per Blanchard J; and MLA Issues Paper, above n 58, at [7.30]–[7.31] and n 245.

[218] Text accompanying above nn 109–116.

[219] *Search of Records, Info, & Data Associated with 14 Email Addresses Controlled by Google LLC* 438 F Supp 3d 771 (ED Mich 2020) at 774–775; and Cochrane, above n 9, at 35

[220] *Microsoft Corp v United States Dept of Justice* 233 F Supp 3d 887 (WD Wash 2017) at 915–16; and Cochrane, above n 9, at 35.

Agreement,[221] there are reasons to question their motivation and practical ability to do so:[222] providers may be driven by commercial interests;[223] and they would need to object under United States law, within short timeframes, and may lack sufficient expertise or knowledge about targets.[224]

Even fewer rights protections apply at the end of this process, when data obtained is deployed in United States criminal proceedings. Like New Zealand, the key protection for digital privacy rights in the United States is an *ex post* exclusion remedy under the Fourth Amendment to the United States Constitution.[225] However, while this is traditionally more generously applied there,[226] it will almost always be unavailable for New Zealand persons or TCNs, given United States jurisprudence limiting Fourth Amendment protections to United States persons or others with substantial voluntary connections there.[227] Neither the SCA nor the Privacy Act of 1974 provide an exclusion remedy.[228] Data will be instead be generally admissible even if gathered in circumstances grossly abusive of digital privacy.[229] This already applies to evidence obtained by the United States through MLA,[230] and underscores the significance of the gatekeeping role played by New Zealand courts and others.

The fact that a US-NZ Agreement would prohibit the United States from targeting New Zealand persons is no panacea. Even if this prohibition was fully reciprocal,[231] New Zealand persons' data would still be incidentally collected during United States requests and could then be relatively freely used by its law enforcement.[232] Their ability to directly target TCNs,[233] in circumstances giving no real protection to their digital privacy rights,[234] should independently concern New Zealand. TCNs include a significant number of non-citizen Māori overseas,[235] as well as residents of many of New Zealand's close allies—a US-NZ Agreement may therefore generate international tensions for New Zealand.[236] Moreover, New Zealand itself,

---

[221] Text accompanying above nn 162–164.

[222] See generally Cochrane, above n 9, at 54–55.

[223] Law Commission and MOJ *Review of the Search and Surveillance Act 2012: Issues Paper* (NZLC IP40, November 2016) [**SSA Issues Paper**] at [9.36]–[9.37]. See for example New Zealand Telecommunications Forum "Submission on the Telecommunications (Interception Capability and Security) Bill" (26 June 2013).

[224] See for example Google, above n 46, at [3.4].

[225] *United States v Strieff* 579 US __, __, 136 S Ct 2056 (2016) at 2061; and Cochrane, above n 9, at 32–33. See also Butler and Butler, above n 80, at [29.2.2].

[226] *Williams*, above n 78, at [271]–[279]; and Scott Optican "A Dialogue on Police Search and Seizure in New Zealand and the United States" (2005) 3 Ohio State J of Crim L 257 at 268–271.

[227] *United States v Verdugo-Urquidez* 494 US 259 (1990) at 265–275; and Cochrane, above n 9, at 21–22.

[228] See for example *United States v Clenney* 631 F3d 658 (4th Cir 2011) at 667 (SCA); and *United States v Moreno-Nevarez* No 13-CR-0841-BEN, 2013 WL 5831017 (SD Cal 2 Oct 2013) at *6–*8 (Privacy Act). See also Cochrane, above n 9, at 44–45.

[229] See Cochrane, above n 9, at 41 n 313.

[230] At 44–45 and 50–51

[231] See text accompanying above n 161. Whether this would be permissible under the Human Rights Act 1993 is beyond the scope of this article.

[232] See Cochrane, above n 9, at 21, 38, and 48.

[233] Text accompanying above n 160. See also text accompanying above n 165.

[234] See Cochrane, above n 9, at 52–55.

[235] Te Puni Kōkiri *Ko Te Tatau i a Ngäi Mäori: Every Mäori Counts* (Fact Sheet 021–2012, November 2012) 021 – 2012 at 4. See also text accompanying below nn 250–259.

[236] See Costi above n 36, at 413; and *Brannigan*, above n 44, at 342.

as well as its service providers,[237] may be liable under the Bill of Rights for United States' acts under a US-NZ Agreement breaching digital privacy: developing jurisprudence suggests public authorities should be responsible for allowing foreign actors to exercise public functions within their territory,[238] such as "coercive powers" to obtain data.[239] Liability would likely arise whether the victim is a New Zealand person or TCN—the Bill of Rights largely protects "everyone".[240] These risks are significant, regardless of how infrequently the United States currently expects to use its new powers.[241] It made the regime expressly reciprocal for a reason. From New Zealand's perspective, a US-NZ Agreement would give the United States unfettered discretion to compel data from New Zealand service providers, absent New Zealand's MLA gatekeepers. As Arnold J noted, writing extrajudicially, "in the exercise of unfettered discretion there is the potential for abuse".[242] This potential is significant.

D *Additional concerns*

New Zealand prides itself on its EU General Data Protection Regulation (**GDPR**) adequacy status,[243] facilitating data transfers between New Zealand and the EU. This will be shortly up for review.[244] To maintain adequacy, New Zealand must provide protections "essentially equivalent" to the GDPR.[245] A US-NZ Agreement may undermine this: in 2020 the Grand Chamber of the Court of Justice of the EU declared that United States law failed to meet this standard;[246] and the GDPR itself requires that its safeguards are "not undermined" during onward transfers of data to third countries.[247] Indeed, the EU has recently questioned the impact of the US-UK Agreement on the United Kingdom's own ability to maintain GDPR

---

[237] See *R v Cox* (2004) 21 CRNZ 1 (CA) at [62]–[65]; *Marsh*, above n 10, at [44]; and *Griffith v R* [2016] NZCA 390 at [37]. See generally *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 2018) at [46]–[47].

[238] Butler and Butler, above n 80, at [5.17]. See also *Alzery v Sweden* (2006) 14 IHRR 341 at [11.6]. See generally *Zaoui v Attorney-General (No 2)* [2005] NZSC 38, [2006] 1 NZLR 282 at [79]; and *Report*, above n 237, at [18], [22], and [25].

[239] *Beaton v Institute of Chartered Accountants of New Zealand* HC Auckland CIV 2005-404-2642, 17 November 2005 at [170]. See generally *Ransfield v The Radio Network Ltd* [2005] 1 NZLR 233 (HC) at [69].

[240] Butler and Butler, above n 80, at [5.10.1]. See generally MLA Issues Paper, above n 58, at [8.104]. See also *TV3 Network Services Ltd v EPCAT New Zealand Inc* [2003] NZAR 501 (HC) at [10]–[15]. But see *Jian v Residence Review Board* HC Wellington CIV-2005-485-1600, 3 August 2003 at [26].

[241] See *US White Paper*, above n 4, at 5; and *UK Explanatory Memorandum*, above n 139, at 5.

[242] Terence Arnold "Why Arrest"? in Roger S Clark (ed) *Essays on Criminal Law in New Zealand* (Wellington: Sweet & Maxwell, 1971) 202 at 214 (quoted in *Neilsen v Attorney-General* [2001] 3 NZLR 433 (CA) at [39]).

[243] Commission Implementing Decision of 19 December 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by New Zealand [2013] OJ L28/12. See generally Regulation 2016/679 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) [2016] OJ L119/1 [**GDPR**] at art 45. See for example (7 August 2019) 740 NZPD 13045 and 13049; and *Naidu v Royal Australasian College of Surgeons* [2018] NZHRRT 23 at [42].

[244] See GDPR, art 45(3).

[245] GDPR, art 45 and recital (104); *Data Protection Commissioner v Facebook Ireland Ltd* EU:C:2020:559, [2021] 1 WLR 751 [*Schrems II*] at [94]; and *Naidu v Royal Australasian College of Surgeons* [2018] NZHRRT 23 at [42].

[246] *Schrems II* at [185].

[247] GDPR, art 44.

adequacy status,[248] leading the UK to delay the US-UK Agreement's implementation while it grapples with "the concrete implementation of [its] data protection safeguards".[249]

New Zealand policy and legislation should also be developed consistently with Māori law principles, including those in Te Tiriti o Waitangi, such as tikanga Māori.[250] Privacy,[251] search and surveillance,[252] as well related areas of New Zealand law,[253] increasingly incorporate Māori law.[254] A "Māori view of privacy" has been articulated, functioning as "both an individual and a collective good".[255] Te Mana Raraunga (the Māori Data Sovereignty Network) also seeks to "enable Māori data sovereignty" by "asserting Māori rights and interests in relation to data" and through recognition that Māori personal data is "a living taonga".[256] The Waitangi Tribunal has further held that New Zealand's electromagnetic spectrum—across which Māori data flows to service providers—is itself taonga.[257] While it is

[248] *Commission Implementing Decision of XXX pursuant to Regulation (EU) 2016 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom* (Draft, 19 February 2021) at (153). See also for example Letter from Andrea Jelinek (Chair of the European Data Protection Board) to Members of the European Union Parliament regarding the US-UK Agreement 1 (June 15, 2020); and European Data Protection Board **[EDPB**] "Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom" (13 April 2021) at [18]–[19] and [88]–[96].

[249] *Commission Implementing Decision*, above n 248, at (143). See also (10 September 2020) 679 GBPD HC 4.

[250] Cabinet Office *Cabinet Manual 2017* at [7.65]; Cabinet Office Circular "Te Tiriti o Waitangi / Treaty of Waitangi Guidance" (22 October 2019) CO (19) 5; and LDAC, above n 8, at 23 and ch 5. See for example *Ngawaka v Ngati Rehua-Ngatiwai ki Aotea Trust Board* [2021] NZHC 291 at [2] and [43]–[47]. See generally Joseph Williams "*Lex Aotearoa*: An Heroic Attempt to Map the Māori Dimension in Modern New Zealand Law" (2013) 21 Waikato L Rev 1 at 34; and Mamari Stephens "Fires Still Burning" Māori Jurisprudence and Human Rights Protections in Aotearoa New Zealand" in Margaret Bedggood, Kris Gledhill and Ian McinTosh (eds) *International Human Rights Law in New Zealand* (Thomson Reuters, Wellington, 2017) 99 at 104–123.

[251] Law Commission, above n 74, at [12.35]–[12.36]. See Privacy Act 2020, s 21(c). See also for example *Tahi Enterprises v Taua* [2018] NZHC 3372 at [157]–[166]; aff'd [2020] NZCA 639.

[252] SSA Report, above n 5, at [2.27]–[2.33] and [2.40]. See *Hamed*, above n 81, at [118], [176]–[178] and [191] per Blanchard J and [232] and [279] per Tipping J. See also for example *Kamo v Minister of Conservation* [2020] NZCA 1 at [28]–[30].

[253] *Takamore v Clarke* [2012] NZSC 116, [2013] 2 NZLR 733 (dead bodies); DNA Report, above n 212, at [2.6] – [2.51]; *Police v Poi* [2018] NZDC 10094 (DNA); and *Re GM* [2018] NZFC 3915, [2019] NZFLR 291 (publication restrictions).

[254] But see Stephens, above n 250, at 123, discussing the "risks of adopting a Eurocentric approach".

[255] Khylee Quince "Māori Concepts and Privacy" in Stephen Penk and Rosemary Tobin (eds) *Privacy Law in New Zealand* (Wellington, 2nd ed, Thomson Reuters, 2016) 29 at 41; and Te Hunga Rōia Māori o Aotearoa "Submission on the Law Commission Search and Surveillance Act 2012 Review" (December 2016) (Obtained on 10 June 2020 under OIA Request to the Law Commission) at [32]–[35].

[256] "Te Mana Raraunga – Māori Data Sovereignty Network Charter" <http://temanararaunga.maori.nz>. See Māui Hudson and others "He Matapihi kit e Mana Raraunga – Conceptualising Big Data through a Māori lens" in H Wahanga, TTAG Keegan and M Appeley (eds) *He Whare Hangarau Māori – Language, culture & technology* (Te Pua Wānanga ki te Ao | Faculty of Māori and Indigenous Studies, the University of Waikato, Hamilton, 2017) 64 at 64–68; and Karaitianga Tairu "Why Data is a Taonga: A customary Māori perspective" (November 2018) <www.tairu.maori.nz>. See generally Joseph A Cannataci *Report of the Special Rapporteur on the Right to Privacy* UN Doc A/73/35712 (17 October 2018) at [72]–[73].

[257] Waitangi Tribunal *The Radio Spectrum Management and Development: Final Report* (Wai 776, 1999) at 42. See Aiden Cameron "Māori Rights in the 4G Radio Spectrum: Fantasy or the Future of Treaty Claims?" (2013) 13 Otago L Rev 181 at 183–184. But see Cabinet Economic Development Committee "Early Access to 5G Radio Spectrum" (9 December 0219) DEV-19-MIN-0329 at [11]–[12].

ultimately "for Māori to say what their interests are" and how these should be protected,[258] a US-NZ Agreement appears to implicate, and potentially undermine, these principles. At minimum, extensive consultation with Māori appears necessary.[259]

V Conclusion

New Zealand should exercise caution. While a US-NZ Agreement would provide benefits, it is not without risks. As the Law Commission noted, a CLOUD Act agreement with the United States—indeed any 'direct access mechanism'—would "involve sacrificing a degree of sovereignty and control over the protection of individuals' privacy in New Zealand".[260] It should not be embarked upon without careful consideration. Ultimately, unless very real concessions can be obtained from the United States, such as removing the reciprocal nature of the regime altogether, its impact on digital privacy and related rights may pose significant and potentially insurmountable concerns.

New Zealand should follow the Australian developments closely. The Australian bill, which has been languishing in its Parliament for over a year, has been extensively criticised on rights grounds similar to those set out here.[261] However, even if Australia proceeds, this should not be seen as a green light for New Zealand, given Australia's contrasting approach to privacy and rights generally.[262]

Overall, New Zealand's relatively robust protections for rights during MLA contrasts with many of its closest security partners, underscoring the importance of New Zealand independently evaluating the appropriateness of these new direct access mechanisms. This is true of the draft Second Additional Protocol to the Budapest Convention:[263] while more constrained than the CLOUD Act regime, its direct access nature nonetheless raises similar concerns.[264] New Zealand should proceed with direct access mechanisms, if at all, only after extensive consideration and full public debate about may be at risk for digital privacy and other rights.

Word count: 12,984 (including footnotes but excluding abstract and identifying author information).

---

[258] Waitangi Tribunal *Ko Aotearoa Tenei: A Report into Claims Concerning New Zealand Law and Policy Affecting Māori Culture and Identity* vol 2 (Wai 262, 2011) at 681.

[259] At 684. See Cabinet Office *Cabinet Manual 2017* at [5.22]; LDAC, above n 8, at 29; and MFAT, above n 8, at 36–38.

[260] SSA Issues Paper, above n 223, at [6.127].

[261] Australian Parliamentary Joint Committee on Human Rights "Human Rights Scrutiny Report" (Report 4 of 2020, 9 April 2020) at 25–26; and Australian Senate Standing Committee for the Scrutiny of Bills "Scrutiny Digest 8 of 2020" (17 June 2020)" at [2.88], [2.92] and [2.95].

[262] See *Finnigan v Ellis* [2017] NZCA 488, [2018] 2 NZLR 123 at [44]–[46]; SSA Issues Paper, above n 223, at [2.54].

[263] See n 7 above.

[264] EDPB, above n 248, at [94].