International Journal of Law and Information Technology, 2017, 00, 1–20
doi: 10.1093/ijlit/eax010
Article

OXFORD

Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?

John Selby*

ABSTRACT

Laws requiring data to be hosted within a particular jurisdiction tend to upset existing ideas about how the Internet should work. Some countries, particularly the USA, have labelled such laws as trade barriers. Other countries, such as Russia and China, have claimed they are pursuing legitimate strategies to protect their citizenry. With a particular focus upon the BRICs, this article aims to make an original contribution to this discourse by synthesizing insights from the disciplines of international trade law and internet governance to analyse and separate the rhetoric from the reality of these competing claims. Drawing upon evidence from information leaked by Edward Snowden about the activities of the US National Security Agency, the article argues that underlying these tensions is the battle to retain or reduce the comparative advantage the US has historically enjoyed in economies of scale for its Internet signals intelligence capabilities. Underneath the debate over trade issues, this article argues that data localization laws are being supported by some countries not only as a means to reduce their comparative disadvantage in Internet data hosting, but also to reduce their comparative disadvantage in Internet signals intelligence.

KEYWORDS: data localization, International trade law, cybersecurity, BRICs

INTRODUCTION

While trade over the Internet is rapidly growing, challenges are emerging from the historical separation which has existed between the two fields of trade regulation and internet governance. Decisions made by stakeholders about how to regulate the Internet are being challenged as trade barriers. This article explores one instance of the emerging collision between trade and the Internet: whether policies that require the local hosting of data should be considered trade barriers.

While other scholars have described data localization generally or regionally[1] and provided a detailed study of how different countries around the world have

* Macquarie University, Optus-Macquarie Cybersecurity Hub, Building E4A, Room 325, Sydney, New South Wales, Australia. E-mail: john.selby@mq.edu.au

1 See, for example, Daniel Castro, 'How Much Will PRISM Cost the US Cloud Computing Industry? (2013) *Information and Technology Foundation* <http://www2.itif.org/2013-cloud-computing-costs.pdf>

introduced data localization laws,[2] this article fills a gap in the literature identified by Chandler and Le, when they commented that 'we leave for a later study a crucial additional concern—the fundamental tension between data localization and trade liberalization obligations'.[3]

The section 'The concept of data localization'of this article provides a brief explanation of data localization. Section 'What motivates the Usa to resist foreign countries' proposals for localized data hosting?' explores the rationale underlying opposition to data localization by US-based stakeholders, including the US government. The section 'Limitations on data localization contained in next generation trade agreements' describes how data localization has been contested in five of the next-generation of regional trade agreements: three agreements promoted by the USA which prohibit data localization (and exclude China) and two agreements promoted by China which do not. Section 'Domestic laws implementing data localization' examines successful and failed attempts to introduce data localization policies within domestic legal frameworks in four of the US' largest trade competitors: the BRICs (Brazil, Russia, India and China). The section 'Separating theory and rhetoric from reality' analyses four policy debates about data localization, distinguishing rhetorical claims from underlying realpolitik so as to identify potential reasons why it is such a contested policy issue.

THE CONCEPT OF DATA LOCALIZATION

One of many fundamental assumptions that the Internet has been built upon is universal connectivity, ie that every node can freely communicate with every other node. Another fundamental assumption has been that the network is dumb at the centre and smart at the edges, ie that it is Internet users who control what they do over the Internet, whereas network providers only route traffic between those users without applying further policy controls over the contents of those communications.[4] Data localization is a concept which challenges those assumptions.

Data localization has two meanings. The first is a policy whereby national governments compel Internet content hosts to store data about Internet users in their country on servers located within the jurisdiction of that national government (localized data hosting). The data stored in the local jurisdiction may be either the sole copy of the data or a required local copy of data sent for storage or processing in another jurisdiction. The second form of data localization is a policy, whereby national governments compel Internet service providers to route data packets sent between Internet users located in their jurisdictions across networks located only within their jurisdiction (localized data routing).[5] This article addresses only the first type of data localization.

accessed 18 December 2016; Kuan Hon and others, 'Policy, Legal and Regulatory Implications of a European Only Cloud' (2016) 24 IJLIT 251.

2 Anupam Chander and Uyen Le, 'Data Nationalism' (2015) 64 Emory LR 677.

3 Chander and Le (n 2) 713.

4 Jerome Saltzer and others, 'End-to-End Arguments in System Design' in Amit Bhargava (ed) *Integrated Broadband Networks* (Artech House 1991); Lawrence Lessig, *Code Version2.0* (Basic Books 2006) 38–60.

5 Chander and Le, above n 2, 680.

In this context, data localization challenges the first and second assumptions mentioned above because it requires Internet content hosts to build or rent data centres in specified jurisdictions rather than to be able to choose wherever those data centres might be most logically located (so as to optimize their economic and/or network performance).

Data localization policies can be broad or narrow in scope. Broad data localization laws have general application to all Internet users and data types across all industry sectors. Narrow data localization laws have more limited scope—either upon specific subsets of the population, upon specific subsets of data, or upon specific industry sectors.[6]

Countries around the world have adopted a range of different attitudes towards data localization and can be broken into two main groups: those promoting data localization policies and those opposing it. While a small number of countries (such as Russia and China) have introduced broad data localization policies, a larger number (including Australia and many EU member states) have introduced narrow data localization policies.[7] The US government and its Internet industry stakeholders have led efforts to oppose the spread of data localization policies. These efforts are discussed in more detail below.

WHAT MOTIVATES THE USA TO RESIST FOREIGN COUNTRIES' PROPOSALS FOR LOCALIZED DATA HOSTING?

Unlike its general balance of trade (which has been consistently in deficit for the last few decades[8]), in 2012, the US reported digital exports in 2012 of $US223 Billion versus digital imports of $US106 Billion, giving it a significant trade surplus in its digital industries (which include data hosting services).[9]

There are at least five reasons why the US enjoys a comparative advantage in the hosting of Internet data. First, the early development of Internet technologies gave many of its company's first-mover advantage in their industries.[10] Secondly, the large size of its domestic economy enables those companies to tap into a large demand base to gain economies of scale that are not available to companies based in smaller countries.[11] Thirdly, a concentration of funding sources and experience creates network effects that support developing start-up companies in Silicon Valley (among other places) that stimulates the rapid growth of its most successful technology

6 ibid, 708–13.

7 ibid, 682–708. While EU member states currently have competence over data localisation issues, the EU has proposed a 'Digital Single Market' which could shift that competence to the supranational level.

8 United States Census Office (2016) *US Trade in Goods and Services – Balance of Payments Basis*, <https://www.census.gov/foreign-trade/statistics/historical/gands.pdf> accessed 18 December 2016.

9 United States International Trade Commission (2014) *Digital Trade in the US and Global Economics: Part 2*, 14.

10 For an early review of the literature on first-mover advantage, see: Roger Kerin and others, 'First Mover Advantage: A Synthesis, Conceptual Framework, and Research Propositions' (1992) 56 J Marketing 33; Barry Leiner and others, 'Brief History of the Internet', *Internet Society* <http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet> accessed 18 December 2016.

11 Michael Armbursl and others, 'A View of Cloud Computing' (2010) 53 Commun ACM 50; CNN Money, 'World's Largest Economies' <http://money.cnn.com/news/economy/world_economies_gdp/> accessed 18 December 2016.

companies.[12] Fourthly, US companies, such as Amazon, DigitalOcean, ComCast and Rackspace dominate the global data hosting industry.[13] Fifthly, US-based data centres enjoy lower operating costs than competitors located in many other countries due to US government indirect subsidies that artificially lower electricity costs (which are the largest running cost for data centres).[14]

A secondary benefit to the US of this trade surplus in data hosting is its contribution to the comparative advantage for its government signals intelligence agencies in their economies of surveillance of online data compared to the economies of surveillance for foreign signals intelligence agencies.[15] Simply put, it is much cheaper for the FBI to issue a national security letter[16] compelling a US-based data host to provide access to their data centres than it is for the NSA to gain access to data stored outside of the USA (whether through making/purchasing and deploying a zero-day exploit, tapping a submarine cable, operating a signals gathering station out of an overseas embassy, deploying malware or flying its Tailored Access Operations teams to capture the data in person).[17]

In the aftermath of the Snowden leaks, the governments of a number of countries (such as Russia and Germany) proposed that they would introduce requirements that their citizens' online data be hosted locally within the country.[18] While various arguments were proposed by those governments (such as freedom from foreign surveillance, privacy, supporting their local hosting industries and enhancing domestic surveillance and law enforcement capabilities[19]), such proposals have been criticized: by trade policy practitioners as being barriers to free trade, and by Western internet governance practitioners as risking the 'Balkanization of the Internet'.[20] The Office

12 Martin Kenney, *Understanding Silicon Valley: The Anatomy of an Entrepreneurial Region* (Stanford University Press 2000).

13 Netcraft, 'Hosting Provider Service Count' <https://www.netcraft.com/internet-data-mining/hosting-provider-server-count/> accessed 18 December 2016.

14 The US federal government provided more than $US30Billion per annum in subsidies for domestic energy production between 2010 and 2013: US Energy Information Administration (2015) *Direct Federal Financial Interventions and Subsidies in Energy in Fiscal Year 2013*, xiii <https://www.eia.gov/analysis/requests/subsidy/pdf/subsidy.pdf> accessed 18 December 2016; National Resource Defence Council (2014) *Data Center Efficiency Assessment*, Issues paper: 14-08-A <https://www.nrdc.org/sites/default/files/data-center-efficiency-assessment-IP.pdf> accessed 18 December 2016.

15 After the Snowden Leaks removed the plausible deniability, the NSA enjoyed regarding its actions, foreign intelligence agencies expressed jealousy at their lack of similar capabilities. See, for example, David Meyer (2014), 'German Spies Want $400M to Play Catch-Up with the NSA', *Yahoo Finance* (31 May 2014) <http://finance.yahoo.com/news/german-spies-want-400m-play-085129757.html> accessed 18 December 2016.

16 For evidence of how the FBI has used National Security Letters to gather information from data hosts, see: *Nicholas Merrill v Lynch* (2014) USDC (SDNY), un-redacted decision: <https://yale.app.box.com/v/nicholas-merrill-sdny-decision> accessed 18 December 2016.

17 For a discussion of the electronic gathering capabilities of the NSA, see: Robert Joyce (2016) 'Disrupting Nation State Hackers', *Speech delivered to USENIX Enigma Conference* (28 January 2016) <https://youtu.be/bDJb8WOJYdA> accessed 18 December 2016.

18 Chander and Le, above n 2 677, fn3. As discussed above, on page 713 of their article, Chander and Le explicitly excluded the issue of trade law consequences from their study.

19 ibid.

20 See, for example, Albright Stonebridge Group (2015) *Data Localization: A Challenge to Global Commerce and the Free Flow of Information* <http://www.albrightstonebridge.com/files/ASG%20Data%20Localization%20Report%20-%20September%202015.pdf> accessed 18 December 2016.

of the US Trade Representative responded to these proposals by issuing warnings against such policies[21]

It is not surprising to see the US government push strongly in the next generation of international trade agreements to restrict efforts to implement data localization in other countries. While there may be technical merits to limiting data localization requirements, it is arguable that its domestic economic political interests[22] and surveillance interests are the primary motivating factors behind its forceful advocacy against data localization. This is particularly the case given that the US government has, in the past, required data localization to be implemented within its own borders when reviewing foreign investments being made into the American telecommunications industry.[23]

LIMITATIONS ON DATA LOCALIZATION CONTAINED IN NEXT GENERATION TRADE AGREEMENTS

Stakeholders in the US have not been content to simply ensure that their own government does not introduce data localization laws. Business stakeholders have actively encouraged the US government to frame data localization as a trade issue[24] and to present evidence against the issue during policy debates within Internet Governance institutions, such as ICANN and the United Nations' Internet Governance Forum.[25]

The World Trade Organization's main multilateral trade agreements are the General Agreement on Trade and Tariffs ('GATT'), the General Agreement on Trade in Services ('GATS') and the Trade-Related Aspects of Intellectual Property ('TRIPS'). There have been multiple rounds of negotiations amongst WTO member states over the last two decades, but the WTOs agenda to stimulate the reduction of trade barriers has arguably stalled.[26]

21 Office of the US Trade Representative (2015) *Section 1377 Review on Compliance with Telecommunications Trade Agreements*, <https://ustr.gov/sites/default/files/2015-Section-1377-Report_FINAL.pdf> accessed 18 December 2016.

22 Shamel Azmeh and Christopher Foster, 'The TPP and the Digital Trade Agenda: Digital Industrial Policy and Silicon Valley's Influence on New Trade Agreements' (2016) 7 LSE International Development WPS 16–175.

23 Chander and Le, above n 2 at 732. Footnote 266 of the Chander and Le article lists and links to multiple agreements between US government agencies and US (and non-US) companies requiring data localization.

24 United States International Trade Commission, 'Digital Trade in the U.S. and Global Economies: Part 1' (2013) *4415* USITC Publication 5-2 <https://www.usitc.gov/publications/332/pub4415.pdf> accessed 18 December 2016.

25 After the author raised the issue of internet governance policy colliding with trade policy during his presentation at the United Nations Internet Governance Forum held in Istanbul in 2014 <http://www.intgovforum.org/cms/174-igf-2014/transcripts/1954-2014-09-03-ws10-new-global-visions-room-6> accessed 18 December 2016, subsequent IGFs have increased their focus on the topic. See, most recently: *Workshop 60: Trans-Pacific Partnership: Good or Bad for the Internet*, United Nations' Internet Governance Forum 2016 (Jalisco Mexico 8 December 2016) <https://igf2016.sched.com/event/8huJ/ws60-trans-pacific-partnership-good-or-bad-for-the-internet> accessed 18 December 2016.

26 Simon Lester, 'Is the Doha Round Over? The WTO's Negotiating Agenda for 2016 and Beyond' *Herbert A Stiefel Center for Trade Policy Studies: Report No. 64*, (11 February 2016) <https://object.cato.org/sites/cato.org/files/pubs/pdf/ftb64.pdf> accessed 18 December 2016.

Given the difficulty in reaching agreement on trade issues at a global level, it is not surprising that some nation-states (notably the US) have sought to progress negotiations towards the next generation of trade agreements at the regional level ('Next Generation Trade Agreements'), which are discussed below. While the number of countries involved in those negotiations has reduced as compared to the WTO's multilateral process, the number of industries affected and scope of those next-generation trade agreements has grown when compared to the GATT, GATS and TRIPS agreements.

Data localization has been a topical issue for negotiators during these trade negotiations. Fiver of these next-generation trade agreements are discussed below. Three of those proposed agreements include the USA (but exclude China and Russia). Two of those proposed agreements include China and/or Russia, but currently exclude the USA.

Trans-pacific partnership

The trans-pacific partnership (TPP) emerged out of a lengthy process which began with the signing of a four-party Trans-Pacific Strategic Economic Partnership in 2005.[27] Article 14.13(2) of the TPP Agreement states that 'No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory'. The agreement contains specific exceptions for government and financial services, and narrow general exceptions in Article 14.13(3) for measures designed to achieve legitimate public policy objectives as long as those measures are not: (a) applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; or (b) imposing restrictions on the use or location of computing facilities greater than are required to achieve the objective.

If a Party introduces such a data localization measure, then a covered person or Party could bring a dispute under the Article 28 Dispute Settlement chapter of the TPP.

Within the TPP, there are two sectoral exceptions to the prohibition on data localization: for financial services[28] and for government services.[29] There are also two general exceptions: for privacy and essential security. Unfortunately, there have been no prior decisions about the meaning of privacy within the context of existing WTO agreements (it also exists as an (untested) exception within the GATS), so there is no current WTO-specific decision-making upon which the breadth of the privacy exception under the TPP could be assessed. Similar to the GATT[30]

27 European Parliament, *Briefing: The Trans-Pacific Partnership: Potential Regional and Global Impacts* (2016) <http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/582028/EPRS_BRI(2016)582028_EN.pdf> 6 accessed 18 December 2016.

28 art 14.1(1): Definitions excludes financial institutions and financial services from being 'Covered Persons' for the purposes of Chapter 14.

29 art 14.2(3) excludes government procurement from Chapter 14.

30 World Trade Organisation, *General Agreement on Trade and Tariffs: Article 21 Security Exceptions*, <https://www.wto.org/english/res_e/booksp_e/gatt_ai_e/art21_e.pdf> accessed 18 December 2016.

and GATS[31] national security exceptions, the essential security exception in the TPP[32] is also considered a risky argument for WTO members to rely upon as it is reserved for serious emergencies and risks tit-for-tat claims in other sectors.[33] Consequently, the breadth and availability of these exceptions for data localization within the TPP are uncertain.

The election in late 2016 of Donald Trump as US President has seen a significant change in US trade policy, with the current version of the TPP being rejected. At the time of writing, it is unclear whether these TPP provisions will re-appear in negotiating drafts of future trade agreements proposed by the USA. The ten remaining countries have expressed some interest in potentially continuing negotiations to sign a TPP without US participation (leaving the door open for a future US President to then commit the USA to that agreement).[34]

Transatlantic trade and investment partnership

The Transatlantic Trade and Investment Partnership (TTIP) has been under negotiation for a number of years. Given their very different attitudes towards privacy,[35] it is unsurprising that the USA and EU have been at odds about (amongst many other things) whether and to what extent the TTIP should include provisions relating to the free flow of information/prohibitions on data localization.[36] For example, while a 2015 EU negotiating draft included explicit permission for financial service suppliers to be able to transfer data in and out of countries when offshore data processing was 'necessary in the ordinary course of business', this was to be balanced against requirements that the USA and EU 'adopt appropriate safeguards for the protection of privacy and fundamental rights, and freedoms of individuals, in particular with regard to the transfer of personal data'.[37] The recent election of Donald Trump as US President has created significant uncertainty as to whether further negotiations on the TTIP will occur and whether the TTIP will be concluded in the short-medium term.[38] In May 2017, the EU stated 'TTIP

31 World Trade Organisation, *General Agreement on Trade in Services: Article XIVbis Security Exceptions* <https://www.wto.org/english/res_e/booksp_e/gatt_ai_e/art21_e.pdf> accessed 18 December 2016; Thomas Cottier and Panagiotis Delimatsis, *Article XIVbis Security Exceptions*, <https://www.researchgate.net/publication/228121387_Article_XIV_bis_GATS_Security_Exceptions> accessed 18 December 2016.

32 art 29(2) TPP.

33 Catherine Gibson, 'Essential Security for the United States in TPP and Beyond' (2015) *Kluwer Arbitration Blog* <http://kluwerarbitrationblog.com/2015/12/22/essential-security-for-the-united-states-in-tpp-and-beyond/> accessed 18 December 2016.

34 CNBC, 'TPP Nations Agree to Pursue Trade Deal Without US' (21 May 2017) <http://www.cnbc.com/2017/05/20/tpp-nations-agree-to-pursue-trade-deal-without-us.html> accessed 3 June 2017.

35 See, for example, the decision in Case 362/14, *Maximillian Schrems v Data Protection Commissioner of Ireland* (2015) < http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362> accessed 18 December 2016.

36 Iain Dreyer, 'EU, US Negotiators Officially Drop Aim of Concluding TTIP in 2016' *Euractiv* (7 October 2016) <https://www.euractiv.com/section/trade-society/news/eu-us-negotiators-officially-drop-aim-of-concluding-ttip-in-2016/> accessed 18 December 2016.

37 European Union, 'Transatlantic Trade and Investment Partnership: Proposal for Services, Investment and E-Commerce Text made public by the EU on 31 July 2015, arts 5-33(1) and 5-33(2) <http://trade.ec.europa.eu/doclib/docs/2015/july/tradoc_153669.pdf> accessed 3 June 2017.

38 Julian Borger, 'Transatlantic Trade Deal "Not Realistic" under Trump, German Official Says', *The Guardian* (15 November 2016).

negotiations are now effectively on hold. . . We need some more time to see where we are'.[39]

Trade in Services Agreement

The 23-member (including the EU) Trade in Services Agreement (TISA) is still in the negotiation stage at the time of writing. Article 2(1) of the leaked[40] Draft Electronic Commerce Chapter of the Trade in Services Agreement states 'No party may prevent the transfer, access, processing or storing of information outside that Party's territory if conducted in connection with a business'. Article 2(5) prevents laws designed to limit the ability of intra-company cross-border data flows. Article 9 prohibits members from requiring service providers to use local data services for processing or storage of data.[41] There is an exception in Article 14 permitting members to take steps to protect their 'essential security interests'.

The USA has also proposed that, unlike the TPP, the exception permitting data localization in financial services should not be included in the TISA.[42] In May 2017, the EU trade negotiators noted that 'The talks were put on hold late Autumn 2016. Next steps to be determined'.[43]

As can be seen from the above three trade agreements, the USA negotiating position has been to promote the free flow of data across national borders, with as few restrictions on that flow as possible. After the election in the USA of President Trump, these negotiations have stalled or collapsed, resulting in the USA ceding initiative on trade negotiations to China—which has a very different attitude towards data localization laws and cross-border data flows.

Regional Free Trade Agreements that exclude the USA

Two regional next-generation trade agreements currently being developed exclude the USA are the ASEAN-based Regional Comprehensive Economic Partnership[44] (RCEP) and the Free Trade Area of the Asia-Pacific (FTAAP). The RCEP includes ten ASEAN member nations plus countries that have signed free trade agreements with ASEAN Members, including China.[45] RCEP negotiations began in 2012, but copies of the draft texts do not appear to have been leaked so far.[46] It is unclear

39 European Union, 'Overview of FTA and Other Trade Negotiations' (May 2017), <http://trade.ec.europa.eu/doclib/2006/december/tradeoc_118238.pdf> accessed 3 June 2017.

40 Wikileaks, 'May 2016 TiSA Publication' (25 May 2016) <https://wikileaks.org/tisa/#May%202016%20TiSA%20Publication> accessed 18 December 2016.

41 Tamir Israel, *TISA Annex on Electronic Commerce: A Preliminary Analysis by the Canadian Internet Policy & Public Interest Clinic (CIPPIC)* <https://wikileaks.org/tisa/ecommerce/analysis/Analysis-TiSA-Electronic-Commerce-Annex.pdf>, accessed 18 December 2016.

42 K. Hegarty, 'Briefing: TPP data localisation – Froman's Fix' (7 July 2016) *Trade and Prosperity* <http://www.tradeandprosperity.org/?p=4432#more-4432>.

43 European Union, above n 39.

44 Department of Foreign Affairs and Trade, 'Regional Comprehensive Economic Partnership' (2016) <http://dfat.gov.au/trade/agreements/rcep/pages/regional-comprehensive-economic-partnership.aspx> accessed 18 December 2016.

45 Australia, China, India, Japan and New Zealand.

46 A search of Wikileaks did not reveal any results that contained RCEP source documents. At the time of writing, the only results it produced discussed the RCEP in the context of TISA.

whether the negotiating drafts for the RCEP contain discussion or prohibitions on data localization but, given China's role in the negotiations, it is unlikely to be the case. In mid-2017, the Chinese Government implemented a Cybersecurity Law that contained data localization requirements.[47]

The FTAAP is currently at an even earlier stage of negotiations[48], but is likely to have received a significant boost given the likely failure of the TPP.[49] It is the only one of these next-generation free trade agreements that includes Russia as a negotiating member.[50] Given both China and Russia are negotiating members of the FTAAP, it is particularly unlikely that prohibitions on data localization will be included in this agreement. Rejection of the TPP by the Trump administration in the USA has offered a boost to the chances of the RCEP and FTAAP.

Having discussed the different ways that the next-generation of international trade agreements have dealt with the issue of data localization, the next section of this article examines how a number of national governments have introduced data localization laws within their jurisdictions.

DOMESTIC LAWS IMPLEMENTING DATA LOCALIZATION

In their detailed study of 'Data Nationalism', Chandler and Le have produced a useful summary of the many countries that have enacted broad or narrow data localization laws.[51] Due to their emerging role in challenging US dominance in international trade, this article focuses upon a narrow sub-set of the countries discussed by Chandler and Le, namely the BRICs (Brazil, Russia, India and China). Two of those countries, Russia and China, have introduced broad data localization laws. India has a narrower data localization law, while Brazil's government proposed, but ultimately rejected, a data localization law. Each of these countries' data localization laws is discussed below (in the order of the acronym BRIC).

Brazil's proposed data localization law

In 2011, the Brazilian government began work on a broad Internet regulatory model, the Marco Civil da Internet.[52] In response to the revelations by Edward Snowden of extensive NSA surveillance, in 2014 Brazilian President Dilma Rousseff proposed an amendment to the draft Marco Civil that included provisions that would have required data localization with penalties for breach of up to 10 per cent of the

47 Proskauer, 'A Primer on China's New Cybersecurity Law: Privacy, Cross-Border Transfer Requirements and Data Localization' <http://privacylaw.proskauer.com/2017/05/articles/international/a-primer-on-chinas-new-cybersecurity-law-privacy-cross-border-transfer-requirements-and-data-localization/> accessed 3 June 2017.

48 APEC, 'Lima Declaration on FTAAP' (20 November 2016) <http://www.apec.org/Meeting-Papers/Leaders-Declarations/2016/2016_aelm/2016_Annex%20A.aspx> accessed 18 December 2016.

49 Global Times, 'Know Your FTAAP', *Global Times China* (23 November 2016) <http://www.globaltimes.cn/content/1019808.shtml> accessed 18 December 2016.

50 Tian Chen, 'China, Russia to Push for Free Trade Area in the Asia-Pacific', *Bloomberg News* (19 November 2016) <https://www.bloomberg.com/news/articles/2016-11-20/china-russia-to-push-for-free-trade-area-in-asia-pacific> accessed 18 December 2016.

51 Chander and Le, above n 2, 677.

52 Anupam Chander Chander and Uyen Le, 'Breaking the Web: Data Localization and the Global Internet', *U.C. Davis International Law Center Working Paper 2014-1*, 6.

previous year's revenue generated in Brazil. A coalition of business and civil society interests protesting against this aspect of the proposal resulted in it being removed from the final version passed by the Brazilian Parliament.[53] Those domestic stakeholder concerns were supported by Chandler and Le's study which suggested that the cost of establishing a data centre in Brazil was significantly higher than expected ($63 m versus $41 m in the USA).[54]

While USA business stakeholders have been reported as 'expressing relief' when the data localization proposal was removed by the Marco Civil,[55] those stakeholders have had a very different experience when engaging with the second of the BRICS, Russia. As discussed below, some companies have complied with Russia's demands whilst others have resisted (and some of these have been sanctioned for their non-compliance).

Russian data localization laws

In 2014, the Russian Parliament passed and the President of the Russian Federation signed a law,[56] Article 18(5) of which required that from 1 September 2015 operators collecting personal data about Russian citizens through electronic communications (including over the Internet) must ensure that databases located in the territory of the Russian Federation are used to 'record, systematize, accumulate, store, amend, update and retrieve' that data.[57] The only exceptions are for data which is processed:

- pursuant to Russian law or treaty obligations;
- for the administration of justice or enforcement proceedings
- for the execution of duties by the Russian state or municipal bodies; or
- for journalistic, media, scientific, literary or creative purposes.[58]

While the law does not explicitly prohibit operators from transferring a copy of personal data about Russian citizens outside of Russia for processing abroad, the Russian President's staff circulated a non-binding commentary recommending that such data processing should occur only within Russia and off-shore data copying should not be permitted. However, as this is a non-binding commentary, it is unclear whether Russian courts would adopt the same restrictive interpretation

53 Angelica Mari, 'Companies Brace for Local Data Storage Requirements' *ZDNET* (7 March 2014) <http://www.zdnet.com/article/companies-brace-for-brazil-local-data-storage-requirements/> ; Angelica Mari, 'Brazil Gives Up On Local Data Storage, Demands Net Neutrality' *ZDNET* <http://www.zdnet.com/article/brazil-gives-up-on-local-data-storage-demands-net-neutrality/> accessed 18 December 2016.

54 Chander and Le (n 52) 36–37.

55 United States International Trade Commission, *Digital Trade in the US and Global Economies: Part 2*, 83, fn138 (2014) <https://www.usitc.gov/publications/332/pub4485.pdf> accessed 18 December 2016.

56 Federal Law of 21 July 2014, No 242-FZ, which amends Federal Law 27 July 2006, No 152-FZ (On Personal Data) and two other laws.

57 For a discussion of the development of this law prior to its passage, see Chander and Le (n 52) 21–22.

58 Linklaters, 'Technology, Media and Telecommunications News: Russia – New Data Localisation Law: Current State of Play' (8 December 2014) <http://www.linklaters.com/pdfs/mkt/london/December_2014_NewsletterPDF.pdf> accessed 18 December 2016.

proposed by the Executive. Contradicting the Russian President's staff, the Russian data protection authority's (Roskomnadzor) November 2014 interpretation of the law permitted offshore transfers to countries party to the Council of Europe Convention on Data Protection where prior written consent from the data subject had been received. In August 2015, the Russian Ministry of Telecommunications' unofficial guidance agreed with the interpretation of the Russian Data Protection Authority regarding offshore transfers, clarified that the data localization law would not apply retroactively (ie there was no requirement to repatriate Russian citizen's personal data if it had already been transferred abroad for processing) but added that it regarded an entity outside of Russia operating a website 'aimed at the territory of Russia' would be required to comply with the Russian data localization requirements. If an entity updated or modifies existing data stored offshore, then it would be required to be localized onto servers located within Russian territory.[59]

A website would be regarded as being 'aimed at the territory of Russia' if it:

- is hosted through the Russian ccTLD or gTLDs associated with Russian territory (eg Moscow)
- offers services under a contract within Russia;
- offers advertisements in the Russian language; or
- has other features indicating the Data Operator has intended to include the Russian market within its business strategy.

Data operators are those entities who would be data controllers or data processors. Unlike US privacy law, the legislation has general application and is not sector-specific.

The new legislation also imposes on Data Operators the obligation to process requests under a 'Right to be Forgotten' request received from the Russian Data Protection Authority (the agency that processes and submits requests received from Russian citizens). Failure to comply with the request from the Russian Data Protection Authority may result in that Authority requesting Russian telecommunication's providers to block Internet access by Russians to the non-compliant entity's website.

Enforcement by the Russian Data Protection Authority has been aggressive in its enforcement of the data localization law, having conducted hundreds of compliance inspections in 2015, restricting access to more than 30 websites that had not complied with the Data Protection Law and publishing a roster of more than 1000 websites who were to be audited for compliance in 2016, including large companies such as Facebook and Twitter.[60] Some online businesses (primarily non-US businesses) have been proactive in complying with these data localization requirements, notably

59 Linklaters, 'Technology, media and Telecommunications News: New Guidance on Russian Data Localisation Law' (August 2015) <http://www.linklaters.com/pdfs/mkt/london/August_2015_NewsletterPDF.pdf> accessed 18 December 2016.

Samsung, Lenovo and AliExpress. Whilst some American businesses have not sought to comply, others have—including eBay, Uber and Paypal. The law has also resulted in a surge of business for Russian-based data hosting centres, including those operated by Orange and IXCellerate.[61]

On 10 November 2016, based upon an application by the Russian Data Authority, the Moscow City Court upheld an August decision of the Moscow District Court that, due to its failure to comply with the Data Localization Law's requirements, access to the LinkedIn website would be blocked within Russia.[62] Interestingly, LinkedIn had previous experience complying with data localization laws: to gain access to the Chinese market it complied with data localization laws in that country.[63] While Apple and Google have complied with the Russian Data Localization Law[64], Facebook and Twitter have not yet done so.[65]

India's data localization laws

Unlike Russia and China, the third of the BRICS, India, has not yet implemented a broad data localization law. Instead, its data localization laws have a narrower scope. Based upon the Information Technology Act of 2000, Rule 7 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Data or Information) Rules of 2011[66] has been interpreted by the Ministry of Communications and Information Technology as requiring companies located in India to obtain the consent of Indians before transferring their sensitive personal data or information abroad only if the receiving country has the same level of data protection and only if it is *necessary* for the performance of lawful contracts.[67] The Public Records Act of 1993 also prohibits the transferring of public records out of

60 Anthony Gallia and others, 'Russian Federation: Russia's Personal Data Localisation Law: Expanding Enforcement' (28 April 2016), <http://www.mondaq.com/russianfederation/x/487470/data+protection/Russias+Personal+Data+Localization+Law+Expanding+Enforcement> accessed 18 December 2016.

61 ibid. See September 2015 interview with Alexander Zharov (in Russian): <http://rkn.gov.ru/news/rsoc/news34448.htm> accessed 18 December 2016.

62 This occurred just a few days after Donald Trump was elected as US President. See: Ingrid Lunden, 'LinkedIn is Now Officially Blocked in Russia' *TechCrunch* (17 November 2016) <https://techcrunch.com/2016/11/17/linkedin-is-now-officially-blocked-in-russia/> accessed 18 December 2016; Rozkomnadzor, 'LinkedIn направлена на блокировку операторам связи', 17 November 2016, <https://rkn.gov.ru/news/rsoc/news41615.htm> accessed 18 December 2016 (in Russian - note Google Translate reports that it 'does not have permission to get URL from this server').

63 ibid.

64 Maria Karnaukh, 'Google Ready for New Personal Data Law; Facebook holds off' *Russia Beyond the Headines* (31 August 2015) <https://rbth.com/science_and_tech/2015/08/31/google_ready_for_new_personal_data_law_facebook_holds_off_48869.html> accessed 18 December 2016.

65 Sputnik News, 'Facebook Plans to Keep Russian User Data Out of Russia Servers' (26 August 2015) <https://sputniknews.com/russia/20150826102620590 0/> accessed 18 December 2016.

66 Chander and Le (n 52) 16–19.

67 *Information Technology Act 2000*, No 21, Acts of Parliament, 2000 (India); *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011*, Gazette of India (11 April 2011); Press Note, 'Clarification on Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011' under s 43A of the Information Technology Act 2000, <http://pib.nic.in/newsite/erelease.aspx?relid=74990> accessed 18 December 2016.; Chander and Le (n 2) 694–7.

India except for 'public purposes' without the prior approval of the Central government.[68]

China's data localization law

Unlike India and Brazil, the final BRIC, China, has implemented a broad data localization law. The Standing Committee of the National People's Congress of China passed a Cybersecurity Law on 7 November 2016.[69] Critical information infrastructure facilities are those entities who operate in a range of sectors, which includes (but is not limited to) the energy, transportation, electricity, gas, water, finance, medical or healthcare and social security sectors. Article 37 requires Critical Information Infrastructure Facilities to store locally citizens' personal information and important data that has been collected or generated during business operations in China. Offshore storage and/or processing requires a security assessment by the State Council to determine whether sufficient legitimate business reasons exist.[70] There are significant corporate and individual penalties imposable for non-compliance.[71]

As part of its strategy seeking to inhibit foreign data localization laws, the Office of the US Trade Representative (diplomatically) expressed concern about the data localization requirements under China's new Cybersecurity Law during the 27th USA–China Joint Commission on Commerce and Trade which was held on 21–23 November 2016 in Washington DC.[72]

This law arguably progresses China's goals of increasing its data sovereignty and promoting its local data centre industry.[73] Technology companies have until July 2017 to comply with this new law.

68 *The Public Records Act*, No 69 of 1993 (India), s 4.

69 Standing Committee of the National People's Congress, 2016 Cybersecurity Law (中华人民共和国网络安全法) (7 November 2016) <http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm> accessed 18 December 2016; Unofficial translation: China Law Translate: <http://chinalawtranslate.com/cybersecuritylaw/?lang=en> accessed 18 December 2016.

70 Gabriela Kennedy, 'China Passes Cybersecurity Law' *Mayer Brown JSM: Legal Update Mainland China* (10 November 2016) <https://www.mayerbrown.com/files/Publication/3c8214cb-f3a4-42c8-bc17-bb2f27da9af3/Presentation/PublicationAttachment/c1a4fdf2-9d57-40bb-8a83-c5b5f8902c82/161110-HKGPRC-CybersecurityDataPrivacy-TMT.pdf> accessed 18 December 2016.

71 art 66 empowers government departments to issue correction orders, warnings, fines of RMB50 000 to RMB500 000, to confiscate unlawful gains, order temporary suspensions of business, close down websites, revoke operating permits or cancel business licences. Individuals directly in charge or responsible for the breach may be fined between RMB10 000 and RMB100 000.

72 Office of the US Trade Representative, 'Fact Sheet 27th US-China Joint Discussions' <https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2016/november/us-fact-sheet-27th-us-china-joint>; US-China Economic and Security Review Commission, '2016 Report to Congress' <http://origin.www.uscc.gov/sites/default/files/annual_reports/2016%20Annual%20Report%20to%20Congress.pdf> accessed 18 December 2016.

73 Samm Sacks, 'Testimony Before the US-China Economic and Security Review Commission', (15 June 2015) <http://www.uscc.gov/sites/default/files/Sacks%20Testimony.pdf>; Dana Polatin-Reuben and Joss Wright, 'An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet' Paper presented to the 4th USENIX Workshop on Freedom of Communications on the Internet (7 July 2014); BMI Research, 'China's New Cybersecurity Law: Cementing Data Sovereignty' (17 November 2016) <http://www.bmiresearch.com/articles/chinas-new-cybersecurity-law-cementing-data-sovereignty> accessed 18 December 2016.

Diversity in data localization law outcomes across the BRICs

One interesting question that remains is why the Brazilian government failed in its attempt to pass a data localization law. Another is why the Indian government has not sought to expand its limited public-sector data localization laws to the private sector (despite occasional proposals by some Indian stakeholders that this should occur).

In both cases, one difference to consider is relatively higher influence of the business sector in political decision-making than in China or Russia. Unlike Brazil,[74] India has a significant export-focused information technology services sector which could potentially split any business stakeholder coalition seeking to promote data localization laws.[75] In the case of Brazil, timing may have played a significant role—the effort to promote Internet civil liberties through the Marco Civil helped to foster and energize a supportive coalition of civil society, business and government stakeholders. The simultaneous attempt by the Brazilian government to introduce data localization contradicted the goals of the energized civil society and business stakeholders who were able to exploit the government's sensitivity to the loss of political capital which would have occurred if those stakeholders had exercised their threat to veto the passage of a Marco Civil that included a data localization law.[76] This might be a contributing factor to explain why the proposal to introduce a broad data localization law in Brazil failed, whereas it succeeded in Russia and China. At this stage, these are only conjectures and further empirical research is needed to resolve these questions.

Data localization laws are not just found in the BRICS

Given the discussion above, some readers might think that data localization laws are promoted by developing country governments seeking to protect local industries and/or authoritarian governments. It is important to recognize the fallacy of such a viewpoint: data localization laws can be found in both developed and developing countries. For example, Germany, Denmark, Belgium, Finland, Sweden and the UK require (at least a copy of) financial records to be stored locally. Bulgaria, Poland and Romania require records of gambling winnings and user transactions to be stored locally. Some European countries require government records to be stored locally: Denmark for financial records of government institutions, the UK for NHS healthcare data and the Netherlands for all public records. France requires the localized installation of systems for intercepting telecommunications. Luxembourg

74 Jean Paul Simon, 'The ICT Landscape in BRICS Countries: Brazil, India, China', 2011, *Joint Research Centre of the Institute for Prospective Technological Studies*, European Commission <http://ftp.jrc.es/EURdoc/JRC66110.pdf> accessed 18 December 2016.

75 Zachary Smith, 'Privacy and Security Post-Snowden: Surveillance Law and Policy in the United State and India' (2014) 9 Intercultural Hum Rights LR 137, 189–207.

76 Angelica Mari, 'Brazil Gives Up On Local Data Storage, Demands Net Neutrality' *ZDNET* <http://www.zdnet.com/article/brazil-gives-up-on-local-data-storage-demands-net-neutrality/> accessed 18 December 2016.

and Swedish laws require the data of financial clients to be stored locally.[77] Australia requires electronic health records to be stored locally.[78]

Having identified a range of data localization laws, the next section of this article analyses why different national governments have pursued such opposing agendas when seeking to promote or resist the introduction of national data localization laws.

SEPARATING THEORY AND RHETORIC FROM REALITY

Since David Ricardo in the 19th Century, economic theorists have generally encouraged free trade on the basis that nation-states are better off if they specialize in producing goods and services for export for which they have a comparative advantage as compared to other nation-states.[79] Economists typically also recommend that each nation-state import from other nation-states goods and services for which they are at a comparative disadvantage.[80] While this is a popular theory, in practice nation-states have not consistently acted in accordance with it—especially with regard to goods and services for which they find themselves at a comparative disadvantage. This can lead to interesting situations wherein the same government agency within a country will, in some situations, both advocate and resist arguments based upon Ricardo's free trade principles.[81] The Nobel-Prize winning economist Joseph Stiglitz calls this a system of 'managed trade, not free trade'.[82]

Proponents of data localization laws have typically raised some or all of the following four arguments as justification for their recommendations: (1) data localization provides better information security against foreign intelligence agencies; (2) data localization supports the local technology industry; (3) data localization protects the privacy and security of citizen's data; and (4) data localization supports local law enforcement. Each of these arguments are discussed in more detail below.

77 A useful summary of these sector-specific data localisation laws can be found in: Matthias Bauer and others, 'Unleashing Internal Data flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States' (2016) European Centre for International Political Economy Policy Brief 5–7. <http://ecipe.org/app/uploads/2016/12/Unleashing-Internal-Data-Flows-in-the-EU.pdf> accessed 18 December 2016

78 s 15 *Personally Controlled Electronic Health Records Act 2012* (Cth) <http://www.austlii.edu.au/au/legis/cth/num_act/pcehra2012473/> accessed 18 December 2016.

79 David Ricardo (1817) 'On the Principles of Political Economy and Taxation' in Piero Sraffa (ed) *Works and Correspondence of David Ricardo*, Volume I (Cambridge University Press 1951), 135.

80 Karl Case and Ray Fair, *Principles of Economics* (7th ed, Pearson 2004) 665–84.

81 A classic example of this can be seen in the Office of the US Trade Representative. The USTR is generally pro-free trade—notably with respect to trade in services such as intellectual property and Internet technologies. At the same time, it supports heavy tariffs on sugar which raise US domestic sugar prices well above the global level so as to protect and enrich a relatively small number of sugarcane and sugar beet growers who have made large domestic political donations for more than a century. For a historical discussion of these US sugar tariffs, see Sara Ellison and Wallace Mullin, 'Economics and Politics: The Case of Sugar Tariff Reform' (1995) 38 JL & Econ 335. For a discussion of its continued relevance in the modern era, see: Sharon Friel and others, 'Shaping the Discourse: What has the Food Industry Been Lobbying For in the Trans Pacific Partnership Agreement and What are the Implications for Dietary Health' (2016) 26 Crit Public Health 518, 526; Bryan Riley, 'US Trade Policy Gouges American Sugar Consumers', *Heritage Foundation Backgrounder #2914*, <http://www.heritage.org/research/reports/2014/06/us-trade-policy-gouges-american-sugar-consumers> accessed 18 December 2016.

82 Joseph Stiglitz, 'The Fair Play Debate: Fair Trade' (2008) 95 Natl Interest 19–24, 21.

Data localization provides better information security against foreign intelligence agencies

The Snowden leaks in 2013 removed the plausible deniability that the US government had enjoyed regarding the massive extent to which their signals intelligence gathering capability had been deployed to surveil politicians, businesses and individuals across the globe and within the USA.[83] Undeniable evidence of the National Security Agency's direct tapping of internet traffic and phone calls of foreign world leaders created an opportunity for those leaders to undermine domestic public support in their countries for the US government and to express public outrage against it.[84]

The question is whether these expressions of outrage were genuine or strategic political theatre. Rulers have routinely spied upon each other (including their allies) for thousands of years. While German Chancellor Merkel protested loudly,[85] shortly thereafter it was revealed that her government's own signals intelligence agency had been engaging in similar conduct against the leaders of other countries.[86]

Given the extent of the NSA's capabilities, it is unlikely that implementing data localization in a country would provide complete protection to the citizens of that country. However, even if complete protection was not possible, it is possible that data localization would increase the cost of surveillance of foreign citizens for the NSA (and other foreign intelligence agencies) and reduce the comparative advantage that it currently enjoys in the economies of surveillance as compared to the signals intelligence agencies in other jurisdictions. While this would not have much impact on NSA surveillance of high-value political or business leaders, it could make it more expensive for the NSA to conduct as wide-spread mass surveillance on the citizens of other countries as it currently does.

Data localization supports local industry

The desire to create local jobs by nurturing local businesses operating at a comparative disadvantage to foreign competitors has a lengthy history. Even economic superpowers have resorted to it—a notable example being when the USA pressured Japanese manufacturers to engage in 'voluntary export restrictions' of automobiles into the USA so as to promote the interests of its Detroit-based car manufacturers.[87] When the local industries are not as large or historically entrenched as General Motors, this argument is commonly referred to as the 'infant industry argument'.[88]

83 There have been countless stories published based upon the leaked NSA documents provided by Edward Snowden to Glenn Greenwald and Laura Poitras. For a general introduction, see: Glenn Greenwald, *The Intercept*, <http://www.theintercept.com> accessed 18 December 2016.

84 James Ball, 'NSA Monitored Calls of 35 World Leaders After US Official Handed Over Contacts' *The Guardian* (24 October 2013) <http://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls> accessed 18 December 2016.

85 Eric Kirschbaum, 'Germany Drops Probe into U.S. Spying on Merkel' *Reuters* (12 June 2015).

86 Madeline Chambers, 'Germany Gives Huge Amount of Phone, Text Data to U.S.' *Reuters* (12 May 2015).

87 Steven Berry, James Levinsohn and Arial Pakes, 'Voluntary Export Restraints on Automobiles: Evaluating a Trade Policy' (1999) 89 Am Econ Rev 400.

88 Robert Baldwin, 'The Case Against Infant-Industry Protection' (1969) 77 J Pol Econ 295. The concept of an infant industry argument was first raised by Alexander Hamilton in his 'Report on the Subject of

The challenge with relying upon the infant industry argument for data localization is that data centres do not really employ any significant numbers of staff. As most countries do not produce their own CPUs, motherboards, RAM chips, hard disks or network equipment (China being the obvious exception), requiring data localization and building local data centres does not typically reduce demand for imports of high-tech equipment.

It is possible that implementing data localization might reduce demand for foreign exchange because local businesses and Internet users would not have to pay foreign companies to host their data offshore. However, it is unclear whether (at least in the short term) this would outweigh the increase in imports necessary to build the local data centres.

A significant weakness in this argument is that local data centres are likely to charge higher prices to local businesses and Internet users to store data as compared to the economies of scale enjoyed by the most efficient global data centre operators. Those higher costs would then create downstream comparative disadvantages for local Internet businesses, leading to an overall loss of efficiency in the local economy. [89]

Another weakness in this argument is the issue of whether the local country has the technical capability and infrastructure needed to successfully reliably operate the local data centre(s). Countries with inadequate or unreliable power networks, or those which experience hot summer months, bad weather or earthquakes might face significant hurdles in avoiding significant downtime for their local data centres. If local businesses and Internet users have no other options for their data hosting, such infrastructure failures could significantly hurt the local Internet-based economy.[90]

Data localization protects the privacy and security of citizen's data

Contrary to the arguments proposed by Chander and Le[91] and Hon[92], data localization laws do not require countries to build only a single local data centre. The protections claimed by Chander and Le to be offered by 'sharding' data[93] would still be possible if a country as large as Brazil, Russia, India or China built multiple local data centres. Of course, this would place even more strain upon their electricity infrastructure than constructing a single data centre and gaining the benefits of redundancy would require the purchase of even more imported high-tech components.

Whether or not local data centre operators would be capable of providing a higher level of security to resist cyber-attacks is unknown. Given the rate at which US companies have revealed that they have been victims to cyber-breaches and that attackers continue to have the advantage over defenders when it comes to cybersecurity, it is

Manufactures' presented to the US Congress on 5 December 1791 and was further developed by Friedrich List in his 1841 'National System of Political Economy'.

89 Chander and Le (n 2) 721–30; Kuan Hon and others (n 1) 255.

90 Kate Galbraith, 'Using the Weather to Cool Data Centres' *New York Times* (5 October 2009) <http://green.blogs.nytimes.com/2009/10/05/using-the-weather-to-cool-data-centers/?_r=0> accessed 18 December 2016; Eileen Yi, 'Singapore to Run Data Centre Trials in Hot Climate Conditions' *ZDNET* (30 May 2016) <http://www.zdnet.com/article/singapore-to-run-data-centre-trials-in-hot-climate-conditions/> accessed 18 December 2016.

91 Chander and Le (n 2) 719.

92 Kuan Hon and others (n 1) 265.

93 Chander and Le (n 2) 719.

unlikely that American management or the location of a data centre in the USA makes it somehow less vulnerable to attackers. Chander and Le also failed to recognize that many cyber-criminals have developed relationships with their host governments, so 'hotbeds of cybercrime' and 'hacker's paradise[s]'[94] that implemented data localization might be able to tap into those local repositories of talent to improve the cybersecurity of their local data centres.[95]

Data localization supports local law enforcement

Local law enforcement agencies around the world have often complained about the difficulties they face when trying to identify and arrest cyber-criminals. While Chander and Le recognize that 'there is no reason to suspect that a criminal is more likely to use one telecommunications provider over another'[96], such an argument fails to appreciate the evidence gathering advantages that localized data hosting could offer local law enforcement.

In particular, relevant evidence consists not only of the cybercriminal's own computer(s), but also the local network and service provider's computers that were transited so as to gain access to the victim's computer. For example, if a local victim reports a cyber-crime has been committed against them to local law enforcement, but that local victim's data was stored in the cloud offshore, the local law enforcement officers face the difficulty of gathering evidence from outside of the jurisdiction. Even if they are willing to provide assistance, the foreign cloud provider may still unintentionally impede the investigation by recording and storing logs in non-standard formats, not logging or retaining records of certain data fields that could be particularly useful for the purposes of the investigation, or by simply failing to provide the needed data in a timely manner. On the other hand, local law enforcement can more easily negotiate or set protocols with the management of a local data centre so as to gain access to the needed information in a timely manner.

Whilst Chander and Le note the benefits to law enforcement officials in many jurisdictions that are members of the Convention on Cybercrime, the BRICs are not listed by them as signatories to that Convention and therefore do not gain access to those benefits.[97] While Brazil, India and Russia are signatories to Mutual Law Enforcement Assistance Treaty with the USA, law enforcement officers routinely complain about the length of time it takes to actually receive assistance for requests made under MLATs.[98]

Chander and Le are correct in their argument that data localization laws implemented in repressive countries risk increasing the capabilities of law enforcement

94 ibid 720.

95 See, for example, Fahmida Rashid, '10 Notorious Hackers Who Went to Work for the Man' *eWeek* (7 September 2011) <http://www.eweek.com/c/a/Security/10-Notorious-Hackers-Who-Went-to-Work-for-The-Man-304218> accessed 18 December 2016.

96 Chander and Le (n 2) 732.

97 ibid 733.

98 S Shalini, 'Evaluating MLATS in the Era of Online Criminal Conduct' *Delhi Centre for Communications Governance Working Paper Series 2015-15, No 2* <http://ccgdelhi.org/CCG%20Working%20Paper%20on%20MLAT%20Reform.pdf> accessed 18 December 2016.

and domestic intelligence agencies to target and harass human rights activists and regime opponents.[99] However, those arguments are silent about the relatively recent historical problems that some countries (notably Russia and China) have faced with foreign governments (such as the USA and UK) seeking to undermine their domestic stability through the actions of foreign agents and domestic actors.

In particular, the Chinese government's focus on maintaining domestic 'stability'[100] has to be understood in the context of three hundred years of foreign intervention (starting with the First and Second Opium Wars where a number of countries (including the UK and US) sought to reduce their trade deficits with China by illegally selling highly addictive opium to its citizens[101]). After tensions which had arisen during the Cold War had dissipated in the 1990s and 2000s,[102] in recent years the Russian government has been particularly concerned[103] about how US-supported 'rainbow' revolutions in recent years have destabilized countries such as Ukraine, Slovakia and Libya.[104] The US government's crackdown on domestic civil liberties and increased surveillance of its citizens (and foreigners) after the 11 September 2001 attacks on New York City and Washington DC shows that even western liberal democracies react in a similar fashion when facing external existential threats.[105]

Both the Chinese and Russian governments seek to maintain the stability of their countries. Their intelligence services are powerful domestic stakeholders in achieving those goals.[106] The Snowden leaks revealed just how far other countries' signals intelligence capabilities had fallen behind that of the US government's NSA, ie they were at a comparative disadvantage when it came to electronic surveillance of domestic and foreign threats when compared to the USA.[107] In such a situation, domestic policies (such as data localization laws) which had the potential to lessen the extent of that comparative disadvantage would find support from those intelligence agencies.

99 Chander and Le (n 2) 735–9.

100 See, for example, the Report of the 16th National Congress of the Chinese Communist Party (2002), which argued that 'stability was the prerequisite for reform and development'. For a discussion of how this is implemented through cybersecurity policy, see: Nigel Inkster, 'Chinese Intelligence in the Cyber Age' (2013) 55 Surviv Glob Politics Strat 45.

101 Arthur Waley, *The Opium War Through Chinese Eyes* (Routledge 1958 (reprinted 2013)); John Haddad, *America's First Adventures in China: Trade, Treaties, Opium and Salvation* (Temple University Press 2013).

102 For a general introduction to this complex topic, see: Graeme Gill and James Young, *Routledge Handbook of Contemporary Russian Politics and Society* (Routledge 2013).

103 Thomas Ambrosio, 'Insulating Russia from a Color Revolution: How the Kremlin Resists Democratic Trends' (2007) 14 *Democratization* 232; Andrei Soldatov and Irina Borogan, 'Russia's Surveillance State' *World Policy Institute* (2013) <http://www.worldpolicy.org/journal/fall2013/Russia-surveillance> accessed 18 December 2016.

104 See, for example, Sharon Wolchik, 'Putinism Under Siege: Can There Be a Color Revolution?' (2012) 23 J Democracy 63.

105 See, for example, Jan Stanley and Barry Steinhardt, 'Bigger Monster, Weaker Chains: The Grown of the American Surveillance Society' in Ronald Sandler (ed), *Ethics and Emerging Technologies* (Palgrave 2014).

106 Peter Mattis, 'The Analytic Challenges of Understanding Chinese Intelligence Services' (2012) 56 Stud Intell 47; Soldatov and Borogan (n 103).

107 Jason Healey, 'The Cartwright Conjecture: The Deterrent Value and Escalatory Risk of Fearsome Cyber Capabilities' (2016) available at SSRN <https://ssrn.com/abstract=2836206> accessed 18 December 2016; Gordon Carera, *Intercept: The Secret History of Computers and Spies* (Weidenfeld & Nicolson 2015); Pranesh Prakash, 'Indian Surveillance Laws and Practices Far Worse than US', *Yahoo India* (13 June 2013) – Stating 'in 2006-7, India's NTRO tried to Crack into Google and Skype Servers, but Failed'.

Thus, it is unsurprising that the USA would seek to retain its comparative advantage by opposing data localization laws whilst other countries, notably Russia and China, would seek to reduce their comparative disadvantage by supporting data localization laws.

CONCLUSION

Data localization is a complex international policy issue which straddles the disciplines of Internet Governance and International Trade Law. Given the inconsistent application in their trade practice by nation-states of Ricardo's trade theory of comparative advantage, it is unsurprising that countries such as the USA (which would suffer both harm to its twin comparative advantages in data hosting services and Internet signals intelligence surveillance) have opposed attempts by other national governments to introduce data localization laws. In particular, the US government has sought to achieve its goal to prevent the spread of such laws by including prohibitions on data localization within the draft texts of the next-generation of regional trade agreements, such as the TPP and TISA.

In contrast, some nation-states (notably Russia and China) at a comparative disadvantage in Internet services, such as data hosting, have supported the introduction of data localization laws. Nation-states who perceive themselves to be at a comparative disadvantage in the efficiency of their Internet signals intelligence are also likely to promote data localization, especially if their governments feel that domestic stability may be undermined within their jurisdictions without it.

To gain a systemic understanding of this issue, further detailed comparative interdisciplinary research is needed to clarify the complex interplay between domestic stakeholders and international factors that have led different countries to adopt different positions on data localization.