*PA*rtecipazione e *CO*nflitto
** The Open Journal of Sociopolitical Studies*
http://siba-ese.unisalento.it/index.php/paco
ISSN: 1972-7623 (print version)
ISSN: 2035-6609 (electronic version)
***PACO*, Issue 11(2) 2018: 511-527**
DOI: 10.1285/i20356609v11i2p511

Published in July 15, 2018

SYMPOSIUM/4

THE POLITICAL ECONOMY OF DATA LOCALIZATION

Jyoti Panday[1]
Electronic Frontier Foundation

Jeremy Malcolm
Prostasia Foundation

1. Introduction

A cliché of our times is that data are the new oil. What felt like a hyperbole even a few years back, today, feels like an apt reference to the commercial and extractive logics of the emerging information economy. The emergence of the data-driven economy defines a disruptive inflection point in the progress of economic globalization (Rodrik 2018). Digital technologies have not only created new modes of trade in goods and services, but they are transforming economic activities in "old economy" sectors like finance, health, logistics, and goods manufacturing. Industries in these sectors rely on cross-border data flows in order to monitor production systems and supply chains, manage global workforces, and provide customer services (Ciuriak and Ptashkina 2018). A report by the McKinsey Global Institute estimates that data-driven artificial

[1] Corresponding author: Jyoti Panday, pandayjyoti@gmail.com

intelligence (AI) technologies deployable now would create between $3.4 and $4.8 trillion annually in value for companies, with biggest potential gains in the areas of sales and supply chain management (Chui *et al*. 2018).

During the early days of the Internet, free data flows were a default consequence of the largely unregulated state of that open, global network (Meltzer and Lovelock 2018). Over time, the digital transformation has expanded the volume of information and categories of data that are collected and processed (Manyika *et al*. 2016), increasingly giving rise to conflicts with national laws and prompting concerns from regulators. In this data-driven economy companies see data as a lucrative asset or a resource that has economic value and can be used to generate profits. Governments build the case for using data to reform existing governance systems and to usher in accountability, transparency and innovation. As data become integrated in knowledge and economic production, contestations around them are defining regulatory interventions and experimentation. The complexity of online data flows has also increased over time. Data are copied, cached, sliced into small portions and distributed across multiple jurisdictions, adding to the complexities of securing control over their flows.

The need to keep pace with the collection, control and movement of data flows has led governments to implement policies that are dramatically shaping the future of the Internet and digital trade. Given the impact of data governance on privacy, security and innovation policies, data localization measures or conditions restricting cross-border data flows have become a prominent issue. This contribution attempts to unpack the politics driving data localization demands particularly in the Asia-Pacific region. In the next section, we explore the categories of information that are being included under localization mandates. In section 3, we provide a preliminary categorization of the structural and policy interventions for localizing information flows and storage that are being adopted by governments around the world. The final section examines how localization measures can be balanced with human rights and the other policy interests associated with unrestricted data flows.

2. Classifying data localization and barriers to data flows

In 2014, cross-border data flows were estimated to have contributed $2.8 trillion to the global economy, a figure expected to reach $11 trillion by 2025 (Kornbluh 2016). The flow of information across international borders creates regulatory complexities, as the data and its subjects, processors and controllers may be subject to laws in multiple jurisdictions.

Data localization refers to the practice of limiting storage, movement and/or processing of data to specific geographies. Countries across the globe are increasingly crafting regulatory frameworks for data and the result is a patchwork of laws and policies that impact corporate data governance as well as individual privacy and other rights and interests. Although all data localization policies are aimed at establishing national control over data, the intensity of such measures can vary from lighter regulations, such as maintaining local copies of data, to outright prohibitions on data transfers.

The more restrictive the conditions stipulated for transferring data overseas, the higher the barrier to digital trade thereby created. Under the most restrictive data regimes, there are multiple and overlapping conditions that must be fulfilled, such as security standards, government approval or strict requirements on consent.

Broadly speaking, data localization policies are developing around two categories of data: commercial and government data.

2.1 Commercial Data

The last few years have seen an emergence of laws that require private sector companies to store commercial data locally. An analysis of fifty data localization restrictions in 21 EU Member States found that most of the restrictions across multiple sectors often applied to commercial data such as accounting documents, tax records, and company records (Bauer *et al*. 2016). Belgium, Denmark, Germany, UK and Finland are some of the countries that require companies to store such commercial data locally.

Similarly, New Zealand requires companies to store certain information such as company records and accounts and to delete copies after a specified duration (Cory 2017). In Indonesia, the government has proposed to introduce categories of commercial data to determine how it should be treated under data localization law (Baker 2017). Thus, companies handling commercial data that have been categorized as important or even low-priority may be required to provide access for law enforcement purposes.

Russia's data localization legislation is an example of a stricter data localization law, in that it requires all domestic and foreign companies to accumulate, store, and process personal information of Russian citizens on servers physically located within Russian borders (Federal Law No. 242-FZ 2016). Such location-based restrictions are akin to a "licensing regime", because they allow Russia to provide capital flows to its private sector by charging admission to international corporations (Newton and Summers

2018). This effectively requires those corporations to rent domestic server space and pay local data services firms or risk being blocked outright in the country.

Localization of data can also be incentivized by raising the costs of transferring data to other jurisdictions. For example, some countries outline a variety of security standards and technical protocols that companies must meet in order to move data outside of the country. Korea's Personal Information Protection Act imposes stringent requirements on service providers to provide customers with details about the data transfer, including the destination of the data, and any third party's planned use for the data (Personal Information Protection Act 2011). In Sweden companies store information locally in order to share it with the authorities who have interpreted a requirement to provide "immediate access" as meaning physical access to servers (Selby 2017).

2.2 Government Data

Government data include personal data and other sensitive information such as health, property, social security and e-voting records that do not relate merely to voluntary commercial transactions. Governments typically restrict the movement of such data on grounds of national security, public order, or personal data protection, in order to minimize security risks such as foreign surveillance and attacks on or misuse of data by rogue actors.

China's National Security Law, for example, limits operations and maintenance of "Critical Internet Infrastructure" to mainland China as matter of national and cyber security (Xinhua Insight 2015). Further measures were taken in 2017 to restrict certain cross-border data flows, by requiring foreign companies to conduct a range of privacy, security, and other impact assessments prior to transferring data overseas, requiring them also to obtain the consent of data subjects if that data contains personal information, and by imposing local data storage requirements on operators in loosely-defined "critical information infrastructure sectors" (Cyberspace Administration of China 2017a; 2017b).

Similarly, in 2017, Vietnam's Ministry of Public Security (MoPS) passed a cyber security legislation requiring all foreign online service providers to store data of citizens exclusively in local data centers, and the Brazilian Central Bank has proposed cybersecurity regulations that would prohibit financial institutions from using data processing and cloud computing services based abroad (Business Software Alliance 2017). Such restrictions on data flows are justified arguing that the government needs access to data in order to perform regulatory duties or to uphold security standards.

Another approach that can be observed in government data localization requirements is to avoid broad, sweeping legislation limiting data flows, in favor of tailored conditions and standards of care for data that has strategic value. For example, the Indonesian Government has proposed amending its data localization legislation to create a protected category for strategic data. If the amendment is adopted, providers of a "public service" would need to ensure that military, intelligence and government related information is stored and processed in Indonesia. Under the Indonesian law, public service providers include both government organizations and certain public-facing private sector companies that provide banking, insurance, health, security, industrial services and social services (Connected Asia 2017).

Another more tailored regulation is South Korea's Land Survey Act, which prohibits exporting local mapping data to foreign companies that do not operate domestic data servers (Indian Express 2016). Similarly, India's National Data Sharing and Accessibility Policy requires all data collected using public funds to be stored within the borders of India (National Data Sharing and Accessibility 2013). More recently, the Chinese government has decreed that all scientific data generated by groups and individuals in China must be submitted to government-sanctioned data centers before publication (Normile 2018). While the rules call for open access and data sharing, data involving state and business secrets, national security, the "public interest," or individual privacy are not covered by the open access exemption.

In 2015, India issued guidelines for a cloud computing empanelment process which mandates that all service providers must store data and services locally in order to be accredited for government services (Livemint 2017). In doing so, such provisions use data localization as a barrier to prevent foreign cloud service providers from providing competing services.

3. What is driving demands for data localization?

Data localization rules are not motivated by a single national or private interest. Various simultaneous factors contribute to national strategies on restricting cross-border data flows or establishing controls for transfer of information.

3.1 Data localization for law enforcement purposes

Data localization is sometimes justified as a measure to facilitate criminal investigations by law enforcement agencies (LEAs). When data are held in other

jurisdictions, officials need to rely on the mutual legal assistance treaties (MLATs) processes to obtain access. The MLAT process was envisaged as a cooperation mechanism in exceptional circumstances. Over time, it has proven to be ill-suited to handle large number of requests or provide immediate or time-bound access to critical information. Moreover, controversies around the inadequacies of the MLAT process have grown and countries started unilateral workarounds. Vietnam and Indonesia, for example, justify maintaining data on in-country servers as a corrective measure to counter the inadequacies of the MLAT process.

In the effort of countering countries that restrict data within their borders for LEA access, the U.S. has been exploring ways to provide its agencies with extraterritorial access to information stored outside the country – as it was the case in the controversy between the United States and Microsoft (Fischer 2018a). The case was dismissed as moot following the passage of the Clarifying Overseas Use of Data (CLOUD) Act in March 2018, which expands American and foreign law enforcement agencies' ability to target and access people's data across international borders (Ruiz 2018). The CLOUD Act gives unlimited jurisdiction to U.S. law enforcement over any content, metadata, and subscriber information controlled by a service provider, regardless of where the data is stored and who created it (Fischer 2018b).

3.2 Protection of individual data

Concerns about the lack of control over collection of personal data and its processing and storage in jurisdictions with autocratic governments, a weak rule of law, or surveillance programs have led governments to recognize data protection as a legitimate reason to limit transfer of data. Countries may mandate data localization to ensure that they are able to enforce their domestic data protection standards over that data. For example, Canada and Australia are among the countries that restrict transfer, storage and processing of personal and sensitive data in other countries that do not have adequate data protection or privacy standards (Schooff 2017).

Indonesia and South Korea have laws that mandate that personal information in the custody of a public body or telecommunications or online service provider be stored and processed only in data centers and disaster recovery centers located in the country (Panday 2017). South Korea's legislation also imposes significant penalties including heavy fines of up to three percent of their revenue for service providers that transfer personal data cross-border without consent. Thailand and Philippines have separate data privacy legislation which are not explicit about data localization, but a broader reading of such laws could see them being used to justify a data localization

requirement (Gnanasagaran 2018). Malaysia is also contemplating a legal framework for the cross-border transfer of personal data (Personal Data Protection Order 2017).

The European Union's (EU) General Data Protection Regulation (GDPR), which came into effect in May 2018, prevents transfer of personal data to jurisdictions not deemed to have adequate privacy protections. The data standards introduced by GDPR apply to the data of EU citizens regardless of where data are held.

There is no agreement on where to draw the line between data protection-based restrictions on data flows that are protectionist and against trade and liberalization, and those that are necessary to guarantee the rights of citizens. Privacy experts have argued that data protection is qualitatively different from forced localization, and that the issue of data localization for data protection would disappear if nations implemented stronger uniform privacy laws or adopted baseline best practices.

Nevertheless, countries continue to pursue carved-out exemptions for data protection in trade agreements that address data flows. Indeed, the growth of data flows has not displaced the dominance of U.S. firms. To respond to the interrelated challenges of countering U.S. hegemony in Internet-based industries, a number of governments are implementing data localization policies to attract foreign businesses to invest, and to incentivize local businesses to stay. In doing so, these governments pursue localization policy as a tool for investment promotion, and to drive local innovation by creating a competitive advantage or leveling the regulatory playing field for local companies. For example, Vietnam is considering data localization for over-the-top telecommunications service providers as a measure for subjecting them to similar regulations as those governing the operations of domestic telecom infrastructure providers (FTI Consulting 2017).

Similarly, the Reserve Bank of India (RBI) has mandated that all payment system operators set up data storage facilities in India by October 2018. The order lacks clarity on definitions and the applicability of the localization requirements. However, it clarifies that restricting payments within the country is necessary in order to ensure "healthy pace of growth in digital payments" (Reserve Bank Of India 2018). The Indian regulations on localization of payments data appear to follow China's model where foreign entities that meet certain criteria, such as setting up a local presence and hosting their client information domestically, are allowed entry into its huge digital payments industry (Bloomberg 2018).

3.3 GeoPolitics of data

The economic rationale is often not the main reason why some governments attempt restricting data flows. For developing and developed countries alike, leadership in the global digital economy is linked to establishing their claims of technological sovereignty. Technological sovereignty goes beyond the idea of economic competition and builds on the idea that advancements in the technological capacity of one nation threaten the national sovereignty of another. This stems from the growing perception that nations that are able to localize technological development and control data flows will fare better in the Internet governance order.

China is the most prominent proponent of localizing technological advancements, where the basic concept of cybersecurity is state-centric and focused on safeguarding the regime against internal and external threats. For over a decade, China has demanded foreign corporations turn over data, but its latest 2017 Chinese cybersecurity regulation tightens the requirements and blacklists corporations who fail to comply. The cybersecurity law extends data localization beyond China's sovereign borders as it defines the notion of territory not only based on the company's nation of incorporation or principal sites of operations and management, but also of ownership (Leyden 2017).

In 2017, Chinese President Xi Jinping revealed his vision of cyber sovereignty which emphasized information control to "oppose and resist the whole range of erroneous viewpoints" (BBC 2017). China has accordingly been steadily increasing data processing costs and logistical challenges for foreign companies (Aaronson 2018), and in May 2017, released detailed standards relating to the protection of personal information (Kennedy and Chen 2018).

Localization measures can also influence public opinion of governments in power, and those seeking re-election. In his annual address to the nation on the eve of the 2018 Russian presidential election, Russian President Vladimir Putin linked technology to national power and prestige, where "lag and dependence translate into reduced security and economic opportunities of the country and, ultimately, the loss of its sovereignty" (Ewing 2018). Russia also maintains a strict focus on domestic information controls while simultaneously expanding data localization policies beyond national borders.

Over time, data sovereignty has gained a more prominent place in the hierarchy of Russian state policy. As of 2015, all data collected on Russian citizens by foreign and domestic companies must be stored and processed on servers in Russia. Russia's far-reaching approach to information controls includes an integration of technical,

personal, financial, social and psychological components (Russia Times 2016). China and Russia have also demonstrated mutual support of their respective sovereignty in cyberspace by entering a bilateral "non-aggression pact" (Korzak 2015).

Asia Pacific countries like Malaysia, Vietnam, Singapore and Thailand have their own competing national interests that guide their approach to regulation of data flows. South Korea, Japan, New Zealand and Australia with diverging policy goals add to the complexity of emerging data regulations in the region. In India protection of national sovereignty over information or reigning in data colonization by U.S. firms has been invoked to drum-up support for introducing rules limiting transfer of data (Venkatesan 2018).

As the above examples demonstrate, the geopolitics of data flows influence localization policies in different ways. While restricting data flows is publicly justified as an economic strategy, such measures can also have political and social implications because they affect public opinion and power. In this larger context, whether data localization is enforced as a form of taxation, or to increase competition, or is viewed as a trade barrier may be a secondary consideration for the government imposing such measures.

Given the increasing importance of data in the digital economy, it is hard to imagine governments letting go of localization as a policy tool. In the absence of global rules or norms for the digital economy, competing national frameworks have become the dominant force shaping the cross-border flow of information online. In the effort of bringing some order to these arrangements and to counter disadvantageous national practices restricting data flows, some governments are exploring data regulation through trade agreements.

4. Human Rights Implications

Data localization or restrictions on movement of data are primarily understood in terms of their economic value or as a geopolitical strategy that helps nations consolidating information security and sovereignty online. However, it is equally important to think about the consequences of such policies on democracy and human rights particularly in this time of growing public debate about the use and commercialization of individual data.

Often, data localization policies are justified as a way to guarantee citizens' rights over their data and improve information security. In fact, data localization policies can have the opposite effect on security and individual rights. For example, by ensuring that

data on individuals are stored within China, not only these data become subject to Chinese jurisdiction, but access to the servers on which that data is stored also becomes physically available to Chinese LEAs and intelligence operatives, with relevant risks for the freedom of Chinese Internet users (Helft 2007).

Centralizing data in local servers, whether operated by domestic or foreign companies, can also make those data more accessible to domestic surveillance programs, many of which have little oversight. By facilitating access to data for intelligence and law enforcement purposes, forced localization can make data about minority groups, journalists, and activists at risk more accessible to repressive authorities.

In environments where legal frameworks are inadequate and provide weak protections for citizens, data localization is likely to increase the risk of human rights infringements. For example, Russia recently introduced a new facial recognition capability originally aimed at assisting in capturing criminals but which, in fact, is a part of its broader effort to leverage data collection for domestic control (Khrennikov 2017).

China's emphasis on government control of data has enabled it to create a social credit system to track and rate the reputations of individuals and businesses. Individuals are scored based on a range of factors such as financial debt, deviation from state-approved online content, and the scores of others within social networks. The national system is expected to increasingly influence all aspects of life, including loan applications, job prospects, travel, and property ownership (Mistreanu 2018).

The success of data localization policies has also emboldened China to explore more restrictive measures for data control. On January 17th, 2017, China's Ministry of Industry and Information Technology issued a document indicating its intention to limit the use of Virtual Private Network (VPN) technologies within China, in order "to promote the healthy and orderly development" of the Chinese Internet (Ministry of Industry and Information Technology 2017). The rise and entrenchment of data localization as a regional norm has the potential to empower repressive regimes and establish a dangerous precedent for governments to follow.

Susan Aaronson has investigated whether free data flow provisions in trade agreements such as the TPP and NAFTA might not only protect the economic interests of the United States, but also incidentally further a human rights agenda (Aaronson 2017a; 2017b; Aaronson and Townes 2012). She acknowledges, however, the limitations of this approach, including the difficulty of surmounting a defense of data localization rules under the public stability or national security exceptions, and the fact that addressing such rules as a trade dispute doesn't address the impacts of such rules

that are unrelated to trade (such as the use of VPNs to securely communicate from point to point within China).

More fundamentally, many human rights activists are profoundly concerned with the use of trade agreements as a human right enforcement mechanism, given that these agreements are negotiated in a closed and opaque process between negotiators who lack human rights experience, and may not consult widely with those affected by the human rights implications of proposed trade rules (Malcolm 2017).

Besides those who negotiate trade texts, the panelists who adjudicate disputes under those texts also tend to lack subject matter expertise outside of trade law. Just as the environmental movement criticized the WTO over its decision in the Dolphin Tuna cases (Kingsbury 1995), one can well imagine how human rights activists would respond to the outcome of a hypothetical trade dispute that found China's data localization rules permissible on national security grounds.

All in all, more than one compelling case has been made for the use of trade rules to address the adverse human rights impacts of data localization measures. It is quite possible that these rules might survive a trade dispute settlement process, given the possible breadth of the available general exceptions, and the lack of human rights expertise among dispute settlement panelists. In any case, aspects of China's data localization rules that do not relate to trade would not be amenable to resolution through trade dispute settlement.

5. Conclusion

Whether it is justified as a measure for protecting individual rights or pursued as means to establish government control over data, the frameworks for data localization reflect various facets of information controls and Internet governance. Data localization policies may be pursued for a variety of reasons, and the domestic political environment dramatically shapes data localization frameworks. A political economy perspective suggests that politics and economics interact to shape localization measures and other discriminatory practices to restrict information.

While restricting data flows can be an economic strategy, such measures also have political and social implications because they affect public opinion and power. Human rights, too, can be impacted and it is unclear whether trade agreements are sufficient to strike the complicated balance required to address these implications. Even less clear is whether trade dispute settlement under the WTO framework or under bilateral or

plurilateral trade agreements would be an adequate remedy to address the human rights implications of data localization arrangements.

Just as data localization policies pursued for economic reasons also have political and social consequences, the reverse is also true. In this respect, we mentioned the cases of China and Russia using data localization policies for domestic surveillance purposes but also that of the data protection justification for Europe's GDPR. Another important political factor is U.S. hegemony over Internet related services, which has driven data localization moves among U.S. trading partners. All these decisions have economic consequences, as companies with business models that depend on collecting data will migrate to jurisdictions with less regulation (Ingram 2018).

The rise of data localization worldwide suggests that localized data governance arrangements will remain a feature of the shifting political and economic order for the foreseeable future. But while data localization policies may sometimes be well-intentioned, and may even in some cases be necessary, as a broader solution to challenges of the information economy such measures are fundamentally at odds with the characteristics of the Internet as a borderless global network.

Dominant international discourses around data localization, which are centered around the trade dimensions of these measures, do not deal systematically with the complex and interdependent demands of the multiplicity of actors that are involved. Adequately addressing the challenges of the rise of data localization is definitely one of the defining issues in the current Internet governance landscape but it does require discussing and accounting for its economic, political and social dimensions in a more integrated fashion.

References

Aaronson S. (2018), "Artificial Intelligence is Trade Policy's New Frontier." Centre for International Governance Innovation. Accessed April 25th, 2018. https://www.cigionline.org/articles/artificial-intelligence-trade-policys-new-frontier.

Aaronson S. (2017), "What Might Have Been and Could Still Be: The Trans-Pacific Partnership's Potential to Encourage an Open Internet and Digital Rights", *Journal of Cyber Policy* 2(2):232–254.

Aaronson S. (2017), "A Comprehensive Approach to Digital Trade Provisions in NAFTA 2.0". https://www.cigionline.org/sites/default/files/documents/Paper%20no.154web.pdf

Aaronson S., Townes, M. (2012), "Can Trade Policy Set Information Free?" Accessed

May 30th, 2018. https://ssrn.com/abstract=2189153.

Baker M. (2017), "Data Localization in Indonesia". Accessed April 25th, 2018. https://www.lexology.com/library/detail.aspx?g=8767c33c-fc99-4d64-ab69-471f34b12d0e.

Bauer M., M.F. Ferracane, H. Lee-Makiyama, and E. van der Maler (2016), "Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States", Policy Brief for the European Center for International Political Economy. Accessed May 30th, 2018. http://ecipe.org/app/uploads/2016/12/Unleashing-Internal-Data-Flows-in-the-EU.pdf.

BBC (2017), "China internet: Xi Jinping calls for cyber sovereignty". Accessed May 30th, 2018. http://www.bbc.com/news/world-asia-china-35109453.

Bloomberg (2018), "China Allows Foreigners to Enter $27 Trillion Payments Market". Accessed March 31st, 2018. https://www.bloomberg.com/news/articles/2018-03-21/china-allows-foreigners-to-enter-27-trillion-payments-market.

Business Software Alliance (2017), "Comments on the Brazilian Central Bank's Proposed Regulation on Cybersecurity Policies and the Procurement of Data Processing, Data Storage, and Other Cloud Computing Services". Accessed on March 30th, 2018. http://www.bsa.org/~/media/Files/Policy/Data/11212017CommentsonCentralBankRegulations_English.pdf.

Chui M., J. Manyika, M. Miremadi, N. Henke, R. Chung, P. Nel, and S. Malhotra (2018), "Notes from the AI frontier: Applications and value of deep learning", McKinsey Global Institute. Accessed on June 15th, 2018. https://www.mckinsey.com/global-themes/artificial-intelligence/notes-from-the-ai-frontier-applications-and-value-of-deep-learning.

Ciuriak D., M. Ptashkina (2018), "Started the digital trade wars have: Delineating the regulatory battlegrounds", E15 Initiative. Accessed on May 30th, 2018. http://e15initiative.org/blogs/started-the-digital-trade-wars-have-delineating-the-regulatory-battlegrounds/.

Connected Asia (2017), "Indonesia moves towards comprehensive data law – how will it impact your business?". Accessed on April 25th, 2018. http://www.connectedasia.com/indonesia-moves-towards-comprehensive-data-law-how-will-it-impact-your-business/#_ftn1

Cory N. (2017), "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?", Information Technology and Innovation Foundation. Accessed on January

27th, 2018. https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost.

Cyberspace Administration of China (2017a), "Measures for the Outward Security Assessment of Personal Information and Important Data". Accessed on January 27th, 2018. http://www.cac.gov.cn/2017-04/11/c_1120785691.htm.

Cyberspace Administration of China (2017b), "Regulations on the Safe Protection of Critical Information Infrastructure". Accessed on January 27th, 2018. http://www.cac.gov.cn/2017-07/11/c_1121294220.htm.

Ewing T. (2018), "Inter-Nyet: The Difficulty of Technological Sovereignty in Russia", Lawfare Blog. Accessed on June 30th, 2018. https://www.lawfareblog.com/inter-nyet-difficulty-technological-sovereignty-russia.

Federal Law No. 242-FZ. (2016), "Processing and Storage of Personal Data in the Russian Federation. Changes since September 1, 2015", Ministry of Telecom and Mass Communications of the Russian Federation. Accessed on January 27th, 2018. http://minsvyaz.ru/en/personaldata/.

Fischer C. (2018a), "EFF to Supreme Court: Protect the Privacy of Cross-Border Data", Deeplinks, Electronic Frontier Foundation. Accessed on Accessed on April 25th, 2018. https://www.eff.org/deeplinks/2018/01/eff-supreme-court-protect-privacy-cross-border-data.

Fischer C. (2018b), "The CLOUD Act: A Dangerous Expansion of Police Snooping on Cross-Border Data", Electronic Frontier Foundation https://www.eff.org/deeplinks/2018/02/cloud-act-dangerous-expansion-police-snooping-cross-border-data.

FTI Consulting (2017), "Localization to Fragment Data Flows in Asia". Accessed on April 25th, 2018. http://www.fticonsulting-asia.com/~/media/Files/apac-files/insights/articles/localization-to-fragment-data-flows-asia.pdf.

Gnanasagaran A. (2018), "Data localisation in Southeast Asia", *The ASEAN Post*. Accessed on April 25th, 2018. Accessed on https://theaseanpost.com/article/data-localisation-southeast-asia.

Helft M. (2007), "Chinese Political Prisoner Sues in US Court, Saying Yahoo Helped Identify Dissidents", *The New York Times*. Accessed on Accessed on April 25th, 2018. https://www.nytimes.com/2007/04/19/technology/19yahoo.html.

Indian Express (2016), "South Korea rejects Google's request to use local mapping data due to security concerns". Accessed on June 30th, 2018. http://indianexpress.com/article/technology/tech-news-technology/south-korea-rejects-google-request-to-use-mapping-data-4381760/.

Ingram D. (2018), "Facebook to put 1.5bn users out of reach of new EU GDPR privacy law", The Irish Times. Accessed on April, 25th, 2018. https://www.irishtimes.com/business/technology/facebook-to-put-1-5bn-users-out-of-reach-of-new-eu-gdpr-privacy-law-1.3466837.

Kennedy G., Q. Chen (2018), "China Issues New Standards on Personal Information Security", *Lexology*, April 2018. Accessed May 30th, 2018. https://www.lexology.com/library/detail.aspx?g=277596b1-7cf9-4d77-9452-1b5b9d4c0500

Khrennikov I. (2017), "Moscow Deploys Facial Recognition to Spy on Citizens in Streets", *Bloomberg*, Accessed on April, 25th, 2018. https://www.bloomberg.com/news/articles/2017-09-28/moscow-deploys-facial-recognition-to-spy-on-citizens-in-streets.

Kingsbury B. (1995), "The Tuna-Dolphin Controversy, the World Trade Organization, and the Liberal Project to Reconceptualize International Law", *Yearbook of International Environmental Law*, 5(1): 1-40.

Personal Information Protection Act (2011). Accessed on July 15th, 2018. http://koreanlii.or.kr/w/images/0/0e/KoreanDPAct2011.pdf.

Kornbluh K. (2016), "A New Framework for Cross-Border Data Flows. Cyber Brief". Accessed on July, 15th, 2018. https://www.cfr.org/report/new-framework-cross-border-data-flows.

Korzak E. (2015), "Is This China and Russia's 'Nonaggression Pact' for Cyberspace?", *The National Interest*. Accessed on January, 22nd, 2017. http://nationalinterest.org/blog/the-buzz/china-russias-nonaggression-pact"-cyberspace-13654.

Leyden J. (2017), "China's cybersecurity law grants government 'unprecedented' control over foreign tech", *The Register*. Accessed on March 30th, 2018. https://www.theregister.co.uk/2017/09/01/china_cybersecurity_law_analysis/.

Livemint (2017), "Govt IT data on cloud system must be stored within India: Meity". Accessed on March 30th, 2018. https://www.livemint.com/Industry/OWeeqJSiHwcDFrOH9kJQoN/Govt-IT-data-on-cloud-system-must-be-stored-within-India-Me.html.

Malcolm J. (2017), "Contested Meanings of Inclusiveness, Accountability and Transparency in Trade Policymaking", Internet Policy Review 6(4).

Manyika J., S. Lund, J. Bughin, J. Woetzel, K. Stamenov, and D. Dhingra (2016), "Digital globalization: The new era of global flows", McKinsey Global Institute. Accessed on June 15th, 2018.

https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows.

Meltzer J., P. Lovelock, (2018), "Regulating for a digital economy: Understanding the importance of data flows in Asia", *Brookings Institute*. Accessed on March 30th, 2018.
https://www.brookings.edu/research/regulating-for-a-digital-economy-understanding-the-importance-of-cross-border-data-flows-in-asia/.

Ministry of Industry and Information Technology (2017), "Notice on Clearing and Standardizing the Internet Network Access Service Market". Accessed on March 30th, 2018.
http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757020/c5471946/content.html.

Mistreanu, S. (2018), "Life Inside China's Social Credit Laboratory", *Foreign Policy*. Accessed on June 15th, 2018. http://foreignpolicy.com/2018/04/03/life-inside-chinas-social-credit-laboratory/.

National Data Sharing and Accessibility Policy (2013). Accessed on June 15th, 2018. http://www.dst.gov.in/national-data-sharing-and-accessibility-policy-0.

Newton, M. and J. Summers (2018), "Russian Data Localization Laws: Enriching Security & the Economy". Accessed on June 15th, 2018.
https://jsis.washington.edu/news/russian-data-localization-enriching-security-economy/.

Normile, D. (2018), "China asserts firm grip on research data", *Science Magazine*. Accessed on April 25th, 2018. http://www.sciencemag.org/news/2018/04/china-asserts-firm-grip-research-data.

Panday, J. (2017), "Rising Demands for Data Localization a Response to Weak Data Protection Mechanisms", *Deeplinks,* Electronic Frontier Foundation. Accessed on July 30th, 2018.
https://www.eff.org/deeplinks/2017/08/rising-demands-data-localization-response-weak-data-protection-mechanisms.

Personal Data Protection Order (Transfer Of Personal Data To Places Outside Malaysia), (2017), Public Consultation Paper No. 1/2017. Accessed on July 30th, 2018. http://www.pdp.gov.my/images/pdf_folder/PUBLIC_CONSULTATION_PAPER_1-2017_.pdf.

Reserve Bank Of India (2018), "Storage of Payment System Data". Accessed on April 25th, 2018.
https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11244&Mode=0.

Rodrik, D. (2018), "Populism and the economics of globalization", *Journal of International Business Policy.* Accessed on July 30th, 2018. https://drodrik.scholar.harvard.edu/files/dani-rodrik/files/populism_and_the_economics_of_globalization.pdf.

Ruiz, D. (2018), "Responsibility Deflected, the CLOUD Act Passes", *Deeplinks*, Electronic Frontier Foundation. Accessed on March 30th, 2018. https://www.eff.org/deeplinks/2018/03/responsibility-deflected-cloud-act-passes.

Russia Times (2016), "Vladimir Putin signs new Russian information security doctrine". Accessed on March 30th, 2018. https://www.rt.com/news/369302-putin-russia-information-security/.

Schooff, J. (2017), "Data Localization: Do You Know Where Your Data Is?", *Open Media*. Accessed on March 30th, 2018. https://openmedia.org/en/data-localization-do-you-know-where-your-data.

Selby, J. (2017), "Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?", *International Journal of Law and Information Technology*, 25 (3):213–232.

Venkatesan, R. (2018), "Without strong data law, India will end up as a digital colony of US, Chinese firms". Accessed on April 25th, 2018. https://blogs.timesofindia.indiatimes.com/Musings/without-strong-data-law-india-will-end-up-as-a-digital-colony-of-us-chinese-firms/.

Xinhua Insight (2015), "China adopts new law on national security". Accessed on March 30th, 2018. http://www.xinhuanet.com/english/2015-07/01/c_134372812.htm.

Authors' Information

Jyoti Panday is a tech/policy professional tracking developments in Internet governance with a focus on Asia where she is based. Jyoti has written about privacy, surveillance, cross-border data flows and platform regulation.

Jeremy Malcolm is Executive Director Prostasia Foundation that focuses on evidence-based solutions to the problem of child sexual abuse. Jeremy has over a decade of experience working on issues related to internet governance and advancing human rights.