scripted

Volume 13, Issue 3, December 2016

DATA LOCALISATION AND THE BALKANISATION OF THE INTERNET

Erica Fraser[*]

Abstract

Unrestricted international data flow is of critical importance to economies and people globally. Data localisation requirements interrupt the global flow of data by restricting where and how they may be stored, processed or transferred. Governments are increasingly imposing such requirements to protect the individual rights of their citizens, along with sentiments of national sovereignty and aspirations of economic benefit. However, data localisation requirements are likely to lead to the balkanisation of the Internet, which may threaten those very objectives. This Analysis article provides and introduction to and an overview of the likely advantages and drawbacks of data localisation requirements following the Snowden revelations. Economic, security and individual rights questions are addressed and illustrated with the recent Russian data localisation law.

DOI: 10.2966/scrip.130316.359

[*] LLM Graduate, University of Edinburgh, United Kingdom.

1. Introduction

The global flow of data has become essential to economies and people everywhere.[1] It has enabled development of the digital economy and revolutionary technical innovations.[2] Further, the Internet's borderless nature promotes individual rights by enabling users to engage in information exchange without geographic restriction, allowing the sharing of ideas, political speech, and other forms of expression.[3] Data localisation requirements interrupt the global flow of data by restricting where and how they may be stored, processed or transferred. Governments are increasingly imposing such requirements ostensibly to protect the individual rights of their citizens, while being commingled with sentiments of national sovereignty and aspirations of economic benefit.[4] In practice, however, these requirements are likely to result in the balkanisation of the Internet and adversely affect both individuals' rights and the digital economy, and should therefore be resisted.[5] These very concerns are being realised as recently implemented Russian data localisation laws take effect. This Analysis article will discuss the nature of data localisation requirements and examine their benefits and risks considering the example of the new Russian legislation.

2. Data Localisation Laws

Data localisation laws can encumber data movement across national borders or limit where and by whom they are stored or processed.[6] They can take the form of blanket bans on information leaving a territory or rules requiring information to be stored domestically.[7] Further, some countries have imposed specific restrictions amounting to forced data localisation, such as controls on the transfer of data in specific sectors such as finance or health, strict requirements for obtaining the data subject's consent prior to international data transfer (which is particularly difficult when data from more than one individual are commingled), or burdensome regulatory approvals for international data transfer.[8] Such laws exist in several developed and developing countries in various forms and degrees, including Canada, Vietnam, Indonesia,

---

[1] A Chander and U Lê, "Data Nationalism" (2015) 64 *Emory Law Journal* 677-739, at 721.

[2] U Ahmed and A Chander, "Information Goes Global: Protecting Privacy, Security, and the New Economy in a World of Cross-border Data Flows" (2015) *UC Davis Legal Studies Research Paper Series*, Research Paper No 480 available at http://ssrn.com/abstract=2731888 (accessed 9 Nov 16); J Hill, "A Balkanized Internet? The Uncertain Future of Global Internet Standards" (2012) *Georgetown Journal of International Affairs* 49-58, at 49.

[3] D Castro, "The False Promise of Data Nationalism" (2013) *Info Tech & Innovation Found* available at http://www2.itif.org/2013-false-promise-data-nationalism.pdf (accessed 8 Nov 16), at 10.

[4] C Millard, "Forced Localization of Cloud Services: Is Privacy the Real Driver?" (2015) 2 *IEEE Cloud Computing* 10-15 available at http://ssrn.com/abstract=2605926 (accessed 8 Nov 2016), at 5.

[5] Chander and Lê, note 1 above, at 714.

[6] Hill, note 2 above, at 3; Chander and Lê, note 1 above, at 680.

[7] N Mishra, "Data Localization Laws in a Digital World" (2016) *Public Sphere Journal* 135-158, at 139, available at http://publicspherejournal.com/wp-content/uploads/2016/02/06.data_protection.pdf (accessed 8 Nov 16); Chander and Lê, note 1 above, at 680.

[8] Mishra, note 7 above, at 139; Chander and Lê, note 1 above, at 680; Ahmed and Chander, note 2 above, at 6.

Brunei, Iran, China, Brazil, India, Australia, Korea, Nigeria, and most recently, Russia.[9] Additional countries are actively contemplating introducing data localisation laws.[10] In response to this trend, global companies are increasingly establishing local servers in countries with such requirements.[11]

Data localisation laws are largely aimed at protecting individuals' fundamental rights online in the face of foreign surveillance and widespread privacy violations, as well as providing a competitive advantage to local companies amid the globalisation of the digital economy.[12] While such restrictions have been considered since the advent of international data networks, the recent increase in legislation has been in direct response to Edward Snowden's 2013 disclosures revealing the United States National Security Agency's (NSA) widespread foreign surveillance activities targeting both American and foreign citizens and companies through its PRISM program.[13] Further, the complicity of US companies with the NSA has led some to the conclusion that only domestic firms operating exclusively within national borders should be entrusted with their citizens' data.[14]

3. Technical Considerations

3.1 Balkanisation

The Internet is largely "open, interoperable and unified."[15] It was developed essentially without regard for national borders as data are routed across the network autonomously and automatically via the most efficient paths.[16] Data move from location to location quickly and in a seemingly arbitrary and unpredictable manner, generally without the user's knowledge or consent.[17] That free flow of data across

---

[9] C Bowman, "A Primer on Russia's New Data Localization Law" (2015) Proskauer Privacy Law Blog available at http://privacylaw.proskauer.com/2015/08/articles/international/a-primer-on-russias-new-data-localization-law/ (accessed 8 Nov 16); Mishra, note 7 above, at 139.

[10] J Hill, "The Growth Of Data Localization Post-Snowden: Analysis And Recommendations For U.S. Policymakers And Business Leaders" (2014) *The Hague Institute for Global Justice, Conference on the Future of Cyber Governance* 1-34, at 4, available at http://ssrn.com/abstract=2430275 (accessed 8 Nov 16).

[11] See eg Y Sverdlik "First Two Microsoft Data Centers Coming to Canada in 2016" (2015) available at http://www.datacenterknowledge.com/archives/2015/06/03/first-two-microsoft-data-centers-coming-to-canada-in-2016/ (accessed 8 Nov 16); CBC News, "Amazon Will Open its First Canadian Data Centre in Montreal" (2016) available at http://www.cbc.ca/news/canada/montreal/amazon-aws-montral-data-center-1.3405616 (accessed 8 Nov 16).

[12] C Kuner, "Data Nationalism and Its Discontents" (2014) 64 *Emory Law Journal* 2089-2098, at 2090, 2092, 2097; M Geist, "The Trouble with the TPP, Day 12: Restrictions on Data Localization Requirements" (2016) available at http://www.michaelgeist.ca/2016/01/the-trouble-with-the-tpp-day-12-restrictions-on-data-localization-requirements/ (accessed 8 Nov 16); Opinion of the European Data Protection Supervisor on the Commission Communication on Internet Policy and Governance – Europe's role in shaping the future of Internet Governance (23 June 2014) available at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-06-23_Internet_Governance_EN.pdf (accessed 8 Nov 16), at 10.

[13] Mishra, note 7 above, at 138; Kuner, note 12 above, at 2090.

[14] Hill, note 10 above, at 6, 19.

[15] Hill, note 2 above.

[16] Chander and Lê, note 1 above, at 680; Ahmed and Chander, note 2 above, at 2.

[17] J Daskal, "The Un-Territoriality Of Data" (2015) 125 *Yale Law Journal* 326-398, at 330.

borders has enabled unprecedented technical efficiencies and economies of scale in storing and processing data.[18] For example, a borderless Internet has enabled technical innovations like cloud computing, which spreads data across various data centres to make affordable and convenient on-demand access to a shared pool of processing or storage facilities, while the actual physical location(s) of the data remains largely invisible to users.[19]

The strengthening of national borders through data localisation laws is likely to balkanise the Internet,[20] fragmenting the global network into "various distinct, idiosyncratic '(I)nternets,'" resulting in delays, inefficiencies, and higher costs.[21] If localisation requirements become widespread, the Internet would require significant redesign of its technical architecture and governance structures.[22] Data localisation would also require global service providers to build or rent physical infrastructure in each jurisdiction. The associated costs and administrative burdens may render infeasible the provision of many global services currently taken for granted by Internet users.[23] Moreover, Internet users and businesses active in the global digital economy would find themselves operating in a "complex array of different jurisdictions imposing conflicting mandates and conferring conflicting rights."[24] Companies may particularly be reticent to invest in local infrastructure in developing countries that lack necessary political stability, a sufficient power grid, and/or supporting laws protecting privacy, data protection, and intellectual property, leaving gaps in Internet service in those countries.[25] This prospect has caused widespread concern. For example, the Organisation for Economic Co-operation and Development (OECD) has warned nations against imposing "barriers to the location, access and use of cross-border data facilities and functions" to "ensure cost effectiveness and other efficiencies."[26] The technical drawbacks of localisation requirements would jeopardise the benefits individual users and businesses enjoy from integrating global communications and the digital economy.[27]

---

[18] Castro, note 3 above, at 10.

[19] Chander and Lê, note 1 above, at 681; P Mell and T Grance, "The NIST Definition of Cloud Computing" (2011) *NIST Special Publication 800-145* available at http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (accessed 8 Nov 16).

[20] Ahmed and Chander, note 2 above, at 1; Chander and Lê, note 1 above, at 680.

[21] S Meinrath, "We Can't Let the Internet Become Balkanized" (2013) *Slate* available at http://www.slate.com/articles/technology/future_tense/2013/10/internet_balkanization_may_be_a_side_effect_of_the_snowden_surveillance.html (accessed 8 Nov 16).

[22] Hill, note 10 above, at 4.

[23] Chander and Lê, note 1 above, at 681.

[24] Meinrath, note 21 above.

[25] Mishra, note 7 above, at 148; N Lehrer, "African Datacenters: Understanding Challenges in Emerging Infrastructure in Developing Countries" (2014) available at http://tech.co/african-datacenters-2014-09 (accessed 8 Nov 16).

[26] Organisation For Economic Co-operation and Development (OECD), "OECD Council Recommendation on Principles for Internet Policy Making" (2011) available at http://www.oecd.org/sti/ieconomy/49258588.pdf (accessed 8 Nov 16); Chander and Lê, note 1 above, at 722.

[27] Hill, note 2 above, at 49; Hill, note 10 above, at 4; Mishra, note 7 above, at 142; Chander and Lê, note 1 above, at 728-30.

3.2 Data Security

Data localisation restrictions are promoted as a means to enhance data security, thereby protecting the privacy and security of personal information against non-governmental actors.[28] However, localisation may in fact result in less security. Data security is maintained through best practices and state-of-the art technology. In a best-case scenario, local storage would have no better access to such practices and technologies than leading global companies. In many cases, though, local storage providers may not apply the same rigour as global providers do due to fewer financial resources and less available expertise, less competitive need to draw customers, or the presence of technological restrictions.[29] For example, localisation requirements would make it impossible for local service providers to employ data security techniques on a global scale that would otherwise be accessible through infrastructure available through the Internet such as sharding, obfuscation, and the distributed storage of backup copies.[30] Moreover, centralising vast quantities of information in a limited number of data centres within a jurisdiction creates an enticing target for those seeking illicit access.[31] In light of these weaknesses, businesses may incur legal liability and suffer lower consumer trust as a consequence of being limited to data processing and/or storage to within the borders of jurisdictions with relatively lower levels of data security.[32] Therefore, data are likely more secure in the absence of data localisation laws, where users are able to select from globally competitive service providers.[33]

4. Individual Rights

The protection of fundamental rights in regard to the online transfer and storage of data is a legitimate concern for states.[34] The physical disconnection between the location of data and that of its user at any specific time undercuts the protection of rights laws, the application of which are location-based.[35] Protecting fundamental rights "requires an element of control by state actors that is severely lacking when the breach is committed by the authorities of a third country and where the effect of that breach is ultimately only experienced on the territory of a third country."[36] Therefore,

---

[28] Chander and Lê, note 1 above, at 718.

[29] *Ibid*, 716, 717, 719; J Arlen and B O'Connor, "Xenophobia is Hard on Data: Forced Localization, Data Storage, and Business Realities" (2015) *SecTor* available at http://www.sector.ca/Program/Sessions/Session-Details/xenophobia-is-hard-on-data-forced-localization-data-storage-and-business-realities (accessed 8 Nov 16).

[30] P Ryan, S Falvey and R Merchant, "When the Cloud Goes Local: The Global Problem with Data Localization" (2013) 46 Computer 54-59, at 54, 56; Daskal, note 17 above, at 368.

[31] Chander and Lê, note 1 above, at 719; Kuner, note 12 above, at 2095-96.

[32] Mishra, note 7 above, at 141-42.

[33] Ahmed and Chander, note 2 above, at 6.

[34] Hill, note 10 above, at 5.

[35] Daskal, note 17 above, at 329.

[36] J Rauhofer and C Bowden, "Protecting Their Own: Fundamental Rights Implications for EU Data Sovereignty in the Cloud" (2013) *University of Edinburgh School of Law Research Paper Series No 2013/28* 1-29, at 25 available at https://ssrn.com/abstract=2283175 (accessed 8 Nov 16).

the use of localisation requirements to prevent the transfer of data abroad can be used as a means for protecting the individual rights of citizens.[37]

4.1 Foreign Surveillance

Preventing foreign surveillance is a widespread justification for data localisation laws, which is grounded in the belief that placing data abroad jeopardises security and privacy.[38] This issue has drawn increased attention since Edward Snowden's recent disclosures revealed extensive NSA foreign surveillance operations.[39] As mentioned above, the exposure of the NSA's systematic violations of individual privacy rights drove both public and government opinion in favour of legislation to keep data within national borders to protect individual rights.[40] While the US has attracted much negative attention for its widespread foreign surveillance activities, they are not alone in employing such tactics.[41] With respect to the protection of individual rights, foreign intelligence services' access to information is legitimately concerning as data subjects often do not enjoy the protection of constitutional or other human rights legislation in the surveilling country.[42] Further, data localisation requirements can serve as a public repudiation of foreign governments and complicit companies engaged in such tactics.[43]

It is unlikely that data localisation restrictions will actually limit other countries' ability to conduct foreign surveillance activities. For example, the new Russian data localisation law offers only weak protection from foreign surveillance since copies of data relating to Russian citizens may be transferred internationally and stored on servers outside Russia.[44] Localisation does not prevent surveillance, as physical access to the data storage or processing facilities is not technically necessary in order to conduct surveillance activities.[45] Further, localisation requirements may in fact facilitate foreign surveillance by centralising information in a particular country, thereby allowing agencies to concentrate their surveillance efforts.[46] Even where

---

[37] See eg *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data,* art 25
available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML (accessed 8 Nov 16).

[38] Chander and Lê, note 1 above, at 679-80.

[39] G Greenwald and E MacAskill, "Boundless Informant: The NSA's Secret Tool to Track Global Surveillance Data" (2013) *The Guardian* available at http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining (accessed 8 Nov 16).

[40] Chander and Lê, note 1 above, at 679; N Hopkins, "UK Gathering Secret Intelligence via Covert NSA Operation" (2013) *The Guardian* available at http://www.theguardian.com/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism (accessed 8 Nov 16); G Greenwald and E MacAskill, "NSA Prism Program Taps in to User Data of Apple, Google and Others" (2013) *The Guardian* available at http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (accessed 8 Nov 16).

[41] Greenwald and MacAskill, note 39 above; Chander and Lê, note 1 above, at 715, 717.

[42] Kuner, note 12 above, at 2094.

[43] Hill, note 10 above, at 23.

[44] Millard, note 4 above, at 4.

[45] *Ibid*; Chander and Lê, note 1 above, at 715; Daskal, note 17 above, at 369-70.

[46] Chander and Lê, note 1 above, at 717.

foreign companies are required to localise their data, this may not be sufficient to prevent the enforcement of foreign legal mechanisms.[47] Moreover, while governments denounce foreign surveillance on behalf of their citizens, many of those same governments secretly share intercepted information with others, such as among the members of the Five Eyes community (of which Australia and Canada have imposed data localisation requirements) and bilaterally between Germany's BND and America's NSA (although Germany has been outspoken in criticising the PRISM program, and its leading telecom company is contemplating a localised German-only network).[48] In light of this, localisation is not an effective means of keeping data from foreign intelligence agencies.[49] It has even been argued that localisation requirements may be used by governments as a tactic to maximise bargaining power with the foreign intelligence agencies.[50]

4.2 Domestic Surveillance

Data localisation laws can also be used as a tool for governments to ensure that data are available to domestic law enforcement for investigative and evidence gathering purposes.[51] This is motivated by a fear of the difficulties associated with compelling information from foreign businesses storing or processing data overseas.[52] However, there are reasonable alternatives available to domestic law enforcement to access data such as domestic legal authority to compel companies operating within their borders to disclose information stored abroad, or by relying on bilateral Mutual Legal Assistance Treaties (although there are concerns about the timeliness, effectiveness and protection for individual rights under such agreements).[53] When these mechanisms are unavailable or unsuccessful, data localisation requirements may not be an effective means to ensure that data is available to domestic law enforcement due to difficulties enforcing such laws.[54] Further, employing data localisation laws to facilitate information collection powers over citizens' data can create risks to individual rights where governments may exercise greater coercive power over domestic businesses storing data to circumvent legal protections. Large, global

---

[47] See however *Microsoft v. United States*, where in July 2016, the United States Court of Appeals for the Second Circuit ruled that a warrant issued under Section 2703 of the Stored Communications Act cannot compel American companies to produce data stored in servers outside the United States.

[48] Editors, "'Prolific Partner': German Intelligence Used NSA Spy Program" (2013) *Spiegel Online International* available at http://www.spiegel.de/international/germany/german-intelligence-agencies-used-nsa-spying-program-a-912173.html (accessed 10 Nov 16); F Dohmen and G Traufetter, "Spy-Proofing: Deutsche Telekom Pushes for All-German Internet" (2013) *Spiegel Online Intternational* available at http://www.spiegel.de/international/germany/deutsche-telekom-pushes-all-german-internet-safe-from-spying-a-933013.html (accessed 10 Nov 16); E MacAskill, J Ball and K Murphy, "Revealed: Australian Spy Agency Offered to Share Data about Ordinary Citizens" (2013) *The Guardian* available at http://www.theguardian.com/world/2013/dec/02/revealed-australian-spy-agency-offered-to-share-data-about-ordinary-citizens (accessed 10 Nov 16); Chander and Lê, note 1 above, at 716.

[49] Chander and Lê, note 1 above, at 716.

[50] Hill, note 10 above, at 22.

[51] *Ibid*.

[52] *Ibid*.

[53] Chander and Lê, note 1 above, at 733-735; R Shah, "Law Enforcement and Data Privacy: A Forward-Looking Approach" (2015) 125 *Yale Law Journal* 543-558.

[54] Chander and Lê, note 1 above, at 732.

businesses, on the other hand, are more likely to resist or at least notify data subjects of disclosure demands.[55]

4.3 Political Repression

As mentioned above, the Internet is an important tool for individuals to communicate globally, and has furthered "individual participation in the political process, increased transparency of governmental activities, and promoted fundamental rights."[56] Conversely, information control is central to the operation of authoritarian regimes that derive their authority in part by suppressing adverse information.[57] As such, strict data localisation laws can enable political oppression by bringing information under governmental control and threatening individual rights such as the rights to privacy, data protection, antidiscrimination and freedom of expression, and democratic values.[58] For example, the Vietnamese *Decree on Management, Provision, and Use of Internet Services and Information Content Online* requires that organisations and enterprises "have at least [one] server system in Vietnam serving the inspection, storage, and provision of information at the request of competent authorities" as a means of enforcing its information control and censorship laws banning the provision or use of the Internet to oppose the regime or threaten national security, social order, and safety.[59]

Protection for freedom of expression, including the right to impart and receive information "regardless of frontiers", is established in the *Universal Declaration of Human Rights* and the *International Covenant on Civil and Political Rights*, and affirmed by the EU *Charter of Fundamental Rights*.[60] An open Internet enhances liberty as political dissidents often rely on foreign speech platforms to disseminate information.[61] Data localisation can erode this benefit by preventing dissidents from using foreign-based services or shrinking the services available to citizens, as businesses will be reticent to operate data centres in authoritarian countries with strong state censorship and surveillance laws.[62]

---

[55] Chander and Lê, note 1 above, at 680; Millard, note 4 above, at 5; Hill, note 10 above at, 21-22, 25-26. See also Google, "Transparency Report" available at https://www.google.com/transparencyreport/userdatarequests/legalprocess/#how_does_google_respond (accessed 14 Apr 2016); C Timberg, "Apple, Facebook, Others Defy Authorities, Increasingly Notify Users of Secret Data Demands after Snowden Revelations" (2015) *The Washington Post* available at https://www.washingtonpost.com/business/technology/apple-facebook-others-defy-authorities-increasingly-notify-users-of-secret-data-demands-after-snowden-revelations/2014/05/01/b41539c6-cfd1-11e3-b812-0c92213941f4_story.html (accessed 10 Nov 16).

[56] Hill, note 10 above, at 28.

[57] Chander and Lê, note 1 above, at 735.

[58] Kuner, note 12 above, at 2097; Chander and Lê, note 1 above, at 680, 735.

[59] *Decree on Management, Provision and Use of Internet Services and Online Information (No. 72/2013),* arts 5(1), 24(2) available at http://www.moit.gov.vn/Images/FileVanBan/_ND72-2013-CPEng.pdf (accessed on 10 Nov 16).

[60] *Universal Declaration of Human Rights* (adopted 10 December 1948 UNGA Res 217 A(III), art 19; *International Covenant on Civil and Political Rights* (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171, art 19; *Charter of Fundamental Rights of the European Union*, art 11 available at http://www.europarl.europa.eu/charter/pdf/text_en.pdf (accessed 10 Nov 16).

[61] Ahmed, note 2 above, at 2.

[62] Mishra, note 7 above, at 142; Chander and Lê, note 1 above, at 735; Ahmed, note 2 above, at 2.

While this is usually raised as a concern with respect to authoritarian states, liberal states have also used data controls to undermine the civil rights of their citizens and residents citing security, privacy, law enforcement, and social-economic reasons.[63] This can have a pernicious and long-lasting effect, forming a precedent from which data controls continue or even enlarge. Moreover, it weakens the position of liberal countries to decry authoritarian regimes' information controls.[64]

5. Economic Effects

Data localisation laws are often hailed as a means of boosting domestic economic development; however, there are compelling reasons to believe that data localisation laws could result in adverse economic effects.[65]

5.1 Domestic Economy

Data localisation laws can be a strategy for responding to the "American Internet hegemony" whereby countries aim to provide local businesses with a competitive advantage to increase their share of domestic IT markets otherwise dominated by US IT companies.[66] For example, laws that require domestic data storage also require the establishment of local data centres, with their associated infrastructure investment and local jobs. This incentive may be particularly high where a telecom monopoly exists; for example, the main benefactors of the Russian data localisation law will be Rostec, a state-owned supplier of IT infrastructure and software, and Rostelcom, the monopoly telecommunications provider in Russia.[67]

There is scepticism, however, as to whether data localisation requirements actually benefit domestic economies, as their adoption has correlated to a negative impact on the enacting countries' GDPs.[68] Any economic gains in the domestic economy would likely be limited to a few local enterprises, data centres, and ancillary businesses, with a limited number of new jobs and much of the associated IT equipment likely being imported.[69] Such gains are small compared to the significant harms that would befall

---

[63] Chander and Lê, note 1 above, at 737.

[64] Chander and Lê, note 1 above, at 738; N Saito, "Whose Liberty? Whose Security? The USA PATRIOT Act in the Context of COINTELPRO and Unlawful Repression of Political Dissent" (2002) 81 *Oregon Law Review* 1051-1131, at 1059–60.

[65] Chander and Lê, note 1 above, at 713; Mishra, note 7 above, at 145.

[66] Hill Growth, note 10 above, at 19; Mishra, note 7 above, at 137-138.

[67] Mishra, note 7 above, at 147; J Verge, "Firms Rethink Russian Data Center Strategy, as Data Sovereignty Law Nears Activation" (2015) available at http://www.datacenterknowledge.com/archives/2015/07/21/russian-data-localization-law-spurs-data-center-strategy-changes/ (accessed 10 Nov 16).

[68] M Bauer et al, "The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce" (2013) available at https://www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf (accessed 10 Nov 16); M Bauer et al, "The Costs of Data Localization: Friendly Fire on Economic Recovery" (2016) *ECIPE* Occasion Paper No 3/2014 available at http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf (accessed 10 Nov 16); M Bauer et al, "Data Localization in Russia: A Self-Imposed Sanction" (2015) *ECIPE Policy Brief* No 6/2015. http://www.ecipe.org/app/uploads/2015/06/Policy-Brief-062015_Fixed.pdf (accessed 10 Nov 16).

[69] Chander and Lê, note 1 above, at 722-23.

the remainder of the digital economy.[70] Firstly, introduction of data localisation requirements inevitably results in increased initial and on-going costs for users, including domestic businesses, as local data services incur significant infrastructure, data migration, and service related costs without enjoying the same efficiencies or economies of scale as global businesses.[71] Moreover, services may be unavailable if the associated costs are too high and the markets too small to make offering such services economical.[72] This could prevent domestic businesses from scaling up and participating in the global digital economy, particular in emerging economies that lack the technical infrastructure that is currently available online.[73] Secondly, data localisation laws are expected to reduce access to global services for Internet users if businesses are opt to withdraw from relevant jurisdictions rather than comply.[74] This will hamper the activities of domestic businesses, which may impair innovation and competitiveness by precluding local companies from using and building upon technological advancements, such as global cloud computing platforms.[75] This issue also concerns traditional businesses offering tangible goods and services that benefit from unfettered Internet access.[76] The establishment of local data centres may also have unintended consequences; for example, data centres use a great deal of electricity, which may result in local businesses suffering power scarcities and paying higher power costs, particularly in developing countries.[77]

5.2 International Trade

International trade may also be negatively impacted by data localisation restrictions.[78] Firstly, it may create an avoidance effect whereby businesses eschew providing services in the country, eroding foreign investment.[79] Secondly, data localisation laws may prompt reciprocal protectionism as other countries erect retaliatory trade barriers, harming consumers and limiting domestic companies' ability to expand internationally via the Internet.[80]

Thirdly, data localisation laws may exclude countries from certain multilateral trade agreements that preclude the use of data localisation requirements. By way of example, the recent Trans-Pacific Partnership (TPP) agreement sets out that "(n)o Party shall require a covered person to use or locate computing facilities in that

---

[70] *Ibid*.

[71] I Mihaylova, "Could the Recently Enacted Data Localization Requirements in Russia Backfire?" (2016) *University of St. Gallen Law School Law and Economics Research Paper Series Working Paper No. 2015-07* at 6, 8 available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2629533 (accessed 10 Nov 16).

[72] Chander and Lê, note 1 above, at 723.

[73] *Ibid*, 728.

[74] *Ibid*, 721. See also G Bovt, "Will Data Law Isolate Russia Further?" (2015) *The Moscow Times* available at http://www.themoscowtimes.com/opinion/article/will-data-law-isolate-russia-further-op-ed/529229.html (accessed on 10 Nov 16).

[75] Chander and Lê, note 1 above, at 721, 723, 728.

[76] *Ibid*, 727.

[77] *Ibid*, 721,723.

[78] *Ibid*, 681.

[79] *Ibid*, 726.

[80] *Ibid*, 713,726.

Party's territory as a condition for conducting business in that territory," subject only to limited exceptions.[81]

6. The Russian Example

6.1 Russian Data Localisation Law

Russia is a large and increasingly important market for businesses around the world, and was found to be one of the most connected emerging markets in 2014.[82] Many global businesses have an established presence in the country through Russian users, customers and employees.[83] The significance of the Russian market and the vast breadth of the Russian localisation requirements make its recent data localisation law germane to this discussion, particularly with respect to individual rights and the digital economy.

After considering data sovereignty requirements for several years, in July 2014 the Russian parliament enacted *Federal Law No 242-FZ*, amending *Federal Law No 152-FZ on Personal Data* to include data localisation requirements.[84] Neither the legislation nor its limited accompanying materials contained detailed information regarding the motives or justification; however, Russian officials have stated policy objectives of national security and the protection of Russian citizens' privacy.[85] The new law was originally set to come into force on September 1, 2016; however, in late 2014, its effective date was advanced to September 1, 2015.[86]

Roskomnadzor, Russia's Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications, is responsible for enforcing the legislation. It conducts supervisory activities including audits of operators and systematic monitoring of the Internet.[87] Failure to comply with the localisation

---

[81] Office of the United States Trade Representative, *Trans-Pacific Partnership,* art 14.13 available at https://ustr.gov/trade-agreements/free-trade-agreements/trans-pacific-partnership/tpp-full-text (accessed on 10 Nov 16)*;* Geist, note 12 above.

[82] J Manyika et al, "Global Flows in a Digital Age: How Trade, Finance, People, and Data Connect the World Economy" (2014) available at http://www.mckinsey.com/insights/globalization/global_flows_in_a_digital_age (accessed 10 Nov 16); Bowman, note 9 above.

[83] Bowman, note 9 above.

[84] *Federal Law No 242-FZ of July 21, 2014 On Amending Some Legislative Acts Of The Russian Federation In As Much As It Concerns Updating The Procedure For Personal Data Processing In Information-Telecommunication Networks*, unofficial translation provided by the Austrian Chamber of Commerce available at http://wko.at/ooe/Branchen/Industrie/Zusendungen/FEDERAL_LAW.pdf (accessed 10 Nov 16); D Polatin-Reuben and J Wright, "An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet" (2014) *4th USENIX Workshop on Free and Open Communications on the Internet (FOCI 14)* available at https://www.usenix.org/conference/foci14/workshop-program/presentation/polatin-reuben (accessed 10 Nov 16) at 3; A Savelyev, "Russia's New Personal Data Localization Regulations: A Step Forward or a Self-Imposed Sanction?" (2016) 32 *Computer Law & Security Review* 128-145, at 130.

[85] Mishra, note 7 above, at 137; Savelyev, note 84 above, at 130.

[86] *Federal Law No. 526-FZ*, as cited in N Gulyaeva, M Sedykh and B Cohen, "Russia Changes Effective Date of Data Localization Law to September 2015" (2015) available at http://www.hldataprotection.com/2015/01/articles/international-eu-privacy/russia-changes-effective-date-of-data-localization-law-to-september-2015/ (accessed 10 Nov 16).

[87] Savelyev, note 84 above, at 134; Roskomnadzor Plan for Audits (2016) available at

obligations may lead to consequences against operators including fines, having access to the offending service blocked, and having the operator and the relevant IP address included in a "black list" registry of offenders maintained by Roskomnadzor.[88]

The legislation requires that all operators "ensure the recording, systematisation, accumulation, storage, adjustment (update, modification), extraction of personal data of citizens of the Russian Federation by means of data bases, situated on the territory of the Russian Federation."[89] The statute does not specify how long local storage must persist, which has been interpreted as meaning that it must be stored indefinitely.[90]

6.2 Uncertainty in the Legislation

There is considerable uncertainty with respect to the precise scope of the Russian data localisation legislation.[91] In August 2015, Roskomnadzor's unofficial clarifications, developed in the course of discussions between regulators and stakeholders in the business community, were released.[92] However, it must be noted that the interpretations set out in Roskomnadzor's unofficial clarification do not always coincide with the language of the statute, leaving open the possibility that the implementation may occur in a different manner than was depicted in the clarification.[93] As such, the ambiguities described below create the possibility that the statute could be implemented in a remarkably wide-reaching manner.[94]

Firstly, there is a fundamental difficulty under the statute for operators to determine what data are subject to the law.[95] Distinguishing personal data from non-personal data for data localisation purposes is extremely complex.[96] Moreover, in contrast to

---

https://www.huntonprivacyblog.com/files/2016/01/Plan_dejatel6nosti_CFO222.pdf (accessed 10 Nov 16), cited in English by N Gulyaeva, M Sedykh and B Cohen, "Russia Releases Data Localization Inspection Plan for 2016" (2016) available at http://www.hldataprotection.com/2016/02/articles/international-eu-privacy/russia-releases-data-localization-inspection-plan-for-2016/ (accessed 10 Nov 16).

[88] *Federal Law No 152 of July 27, 2006 on Personal Data*, unofficial translation provided by the Austrian Chamber of Commerce available at http://wko.at/ooe/Branchen/Industrie/Zusendungen/FEDERAL_LAW.pdf (accessed 15 Apr 2016), art 15.5, as amended by *Federal Law No. 242-FZ*, note 84 above, art 1; Savelyev, note 84 above, at 135; Bowman, note 9 above.

[89] *Federal Law No. 242-FZ*, note 84 above, art 2.

[90] Mihaylova, note 71 above, at 6.

[91] Millard, note 4 above, at 3.

[92] Roskomnadzor, Unofficial Clarifications available at http://minsvyaz.ru/ru/personaldata/#1438546984884 (accessed 10 Nov 16) as cited in English by N Gulyaeva, M Sedykh and B Cohen, "Russia Update: Regulator Publishes Data Localization Clarifications" (2015) available at http://www.hldataprotection.com/2015/08/articles/international-eu-privacy/russia-update-regulator-publishes-data-localization-clarifications/ (accessed 10 Nov 16); Savelyev, note 84 above, at 130.

[93] V Shaftan, "Russian Data Protection Authority Explains Data Localization Law; Says Cross-Border Transfer Still Permitted" (2014) available at http://www.dataprotectionreport.com/2015/08/russian-data-protection-authority-explains-data-localization-law-says-cross-border-transfer-still-permitted/ (accessed 10 Nov 16).

[94] Mihaylova, note 71 above, at 5; Savelyev, note 84 above, at 132.

[95] Mishra, note 7, at 141.

[96] Bauer, "Data Localization in Russia", note 68 above.

other countries' data localisation regimes, Russia's law applies to personal data based on citizenship, an unusual distinction compared to more common distinctions based on industry or information type.[97] It is not clear whether the requirement applies to data of Russian citizens located outside of the country.[98] Moreover, most data operators do not know the nationality of their data subjects, and requiring this information is an unnecessary collection of sensitive personal data since citizenship is irrelevant for the provision of most online services.[99] In light of this limitation, Roskomnadzor has suggested that it may substitute data originating in Russia for citizenship; that is, the law will apply to all personal data collected in Russia, presumably including that of non-citizens.[100]

Secondly, the law's application is extremely broad, applying to any entity, local or foreign, that stores or processes the personal data of Russian citizens on foreign servers.[101] The unofficial clarification released by Roskomnadzor states that the law will be construed to apply to foreign entities that purposefully direct activities "aimed at the territory of the Russian Federation" and extracts benefits from such activities. Roskomnadzor has interpreted this to include having a physical presence in Russia, using a Russian domain name, using the Russian language or currency, marketing in Russia, having a Russian contact phone number, or delivering goods and services (including digital) in Russia; however, as this list is not exhaustive, foreign entities may lack certainty as to whether the law applies to them.[102] In order to comply with the law, entities based outside of the country will need to establish local data server facilities in Russia. Some companies with significant business in Russia are doing so, such as Booking.com and Samsung.[103] Others, however, are expected to exit the market.[104]

Thirdly, it is not clear from the statutory language whether operators may transfer personal data abroad; however, international transfers seem to be at odds with the purpose of protecting Russian citizens from foreign surveillance.[105] Roskomnadzor's unofficial guidance states that the statute does not prevent copies of relevant personal

---

[97] Bowman, note 9 above; Mihaylova, note 71 above, at 5; Savelyev, note 84 above, at 132.

[98] Millard, note 4 above, at 3.

[99] Savelyev, note 84 above, at 132.

[100] Letter of Roskomnadzor No. 08АП-3572 of 19 January 2015, § 5, as cited by Savelyev, note 84 above, at 132.

[101] Mihaylova, note 71 above, at 5.

[102] Bowman, note 9 above; Roskomnadzor, Unofficial Clarifications available at http://minsvyaz.ru/ru/personaldata/#1438546984884 (accessed 10 Nov 16) as cited in English by V Shaftan, "Russian Data Protection Authority Explains Data Localization Law; Says Cross-Border Transfer Still Permitted" (2014) available at http://www.dataprotectionreport.com/2015/08/russian-data-protection-authority-explains-data-localization-law-says-cross-border-transfer-still-permitted/ (accessed 10 Nov 16); Savelyev, note 84 above, at 137.

[103] Interview with A Zharov (2015) available at http://rkn.gov.ru/news/rsoc/news34448.htm (accessed 10 Nov 16), cited in English by N Gulyaeva, M Sedykh and B Cohen, "Russian Data Localization: Two Months In" (2015) available at http://www.hldataprotection.com/2015/10/articles/international-eu-privacy/russian-data-localization-two-months-in/ (accessed 10 Nov 2016).

[104] Verge, note 67 above.

[105] Savelyev, note 84 above, at 132.

information being transmitted outside Russia provided it is initially uploaded in Russia and that copy is maintained on a server within the country.[106]

6.3 Associated Risks

Russia's localisation requirements illustrate the associated legal, technical, economic and rights risks to Russian citizens and domestic and global businesses. Firstly, the localisation requirements are expected to have a significant impact on the Russian economy, as well as the global digital economy.[107] Domestically, the law imposes strict localisation requirements that will likely result in users bearing the costs of the localisation scheme, global companies withdrawing from the market, and Russian businesses facing higher barriers to entering the global market.[108] Secondly, requiring that a copy of all personal data be kept on Russian soil risks the security and privacy of Russian personal data whereby a virtual jackpot of data is made available to potential hackers as well as state surveillance organs.[109] Finally, and perhaps most alarmingly, there is significant concern that Roskomnadzor will use the legislation as a tool to repress political dissent through online platforms. Subversive information from the outside world could be supressed via a massive blocking of access to foreign web sites for non-compliance with data localisation provisions, particularly given the possibility that the ambiguities in the legislation could be interpreted in such a way as to make compliance exceedingly difficult.[110] Residents will have fewer platforms on which to exercise freedom of expression, while the prospect of lower barriers to domestic surveillance may have a chilling effect. It has been argued that taken far enough, "Russia may even succeed in splintering the web, breaking off from the global Internet a Russian intranet that's easier for it to control."[111]

7. Conclusion

Given the Internet's borderless nature and the resulting unpredictability of the location of data at any particular time, the lack of consistently high protections for the rights of individuals and their data in every country is legitimately concerning, especially in light of breaches such as Snowden's revelations on the PRISM programme. As such, data localisation requirements are being held up as a means of imposing national ideals and values concerning the protection of individual rights on the Internet.[112] Moreover, the establishment of such laws is in part attributable to populist politics, providing a comforting and easily understood solution to people's fears relating to globalisation and its threats to national or regional identities and values.[113] In practice, however, data localisation laws are unlikely to be effective in achieving their desired purposes – they will not provide absolute protection against

---

[106] Roskomnadzor Unofficial Clarifications, note 102 above; Millard, note 4 above, at 4; Savelyev, note 84 above, at 132.

[107] Bauer, "Data Localization in Russia", note 68 above.

[108] Mihaylova, note 71 above, at 8.

[109] Millard, note 4 above, at 4.

[110] Savelyev, note 84 above, at 135; Mishra, note 7 above, at 137.

[111] A Soldatov and I Borogan, "Russia's Surveillance State" (2013) 30 *World Policy Journal* 23-30, at 24.

[112] Rauhofer, note 36 above, at 25; Castro, note 3 above, at 10; Kuner, note 12 above, at 2095, 2098.

[113] Hill, note 10 above, at 23-24; Kuner, note 12 above, at 2092, 2098.

foreign surveillance and may in fact threaten other fundamental rights like freedom of expression and, in some cases, increase the risk of political repression. Further, localisation requirements risk balkanising the Internet, which would likely nullify technical efficiencies in the network, create greater risks to data security, and harm the digital economy. On balance, given the likely ineffectiveness in accomplishing its objectives and the probably adverse effects to both individuals' rights and the digital economy, data localisation requirements should be resisted. Rather, Internet users should have the right to choose what entities will best protect the security of their data and their rights, regardless of location, informed by transparency on how such entities protect data and cooperate with government surveillance organisations.[114]

[114] Hill, note 10 above, at 26.